

A new enlightenment about gaps between primes

Belhaouari, Samir B.

Department of Computer science, INNOPOLIS University, Kazan, Russia
 Department of Mathematics, University of Sharjah, UAE
 email: samir.brahim@gmail.com

June 16, 2015

Abstract

The idea of generating prime numbers through sequence of sets of co-primes was the starting point of this paper that ends up by proving two conjectures, the existence of infinitely many twin primes and the Goldbach conjecture. The main idea of our approach is summarized on the creation and on the analyzing sequence of sets of distinct co-primes with the first n primes, $\{p_i : i \leq n\}$, and the important properties of the modulus linear combination of the co-prime sets, $H = (1, p_{n+1}, \dots, \prod_{i=1}^n p_i - 1)$, that gives sets of even numbers $\{0, 2, 4, \dots, \prod_{i=1}^n p_i - 2\}$. Furthermore, by generalizing our approach, the Polignac conjecture "the existence of infinitely many cousin primes, $p_{n+1} - p_n = 4$," and the statement that "every even integer can be expressed as a difference of two primes," are derived as well.

Subject Classification: 11A41, 11L20 .

Keywords: Prime number, twin number, Goldbach's conjecture.

Contents

1	Introduction	2
2	Abbreviation and Notation	4
3	Sketch of the proof	5
4	Proof of Theorem 3.1	11
5	Proof of Lemma 3.2	13
5.1	Proof of Lemma 3.2 part (i)	13
5.2	Proof of Lemma 3.2 part (ii)	14

6	Proof of Lemma 3.3	16
6.1	Proof of Lemma 3.3 part (i)	16
6.2	Proof of Lemma 3.3 part (ii)	18
7	Proof of Lemma 3.4	20
8	Proof of Lemma 3.5	23
9	Proof of Lemma 3.6	32
9.1	Proof of the first part of Lemma 3.6	33
9.2	Proof of the second part of Lemma 3.6	33
9.3	Proof of the third part of Lemma 3.6	35
9.4	Proof of the fourth part of Lemma 3.6	36
10	Proof of the conjecture of Goldbach	36
11	Proof of the conjecture of twin prime	38
11.1	First Approach	38
11.2	Second Approach	38
12	Appendix	43

1 Introduction

The proof of the existence of infinitely many twin primes has been one of the most difficult and the oldest question in number theory for several years. The twin prime conjecture states: There are infinitely many primes p such that $p+2$ is also prime. Some attribute the conjecture to the Greek mathematician Euclid of Alexandria, who gave the oldest known proof that there exist an infinite number of primes.

In 1849 de Polignac made the more general conjecture that for every integer k , there are infinitely many prime pairs (p_1, p_2) such that $p_1 - p_2 = 2k$. The twin prime conjecture is for $k = 1$.

Since every three consecutive numbers, $(p, p + 1, p + 2)$, are not all co-primes with the number 3, then 2 and 3 are factors of $p + 1$. Subsequently, all twin primes are in the form of $6n \pm 1$ except for the first pair $(3, 5)$ and also all cousin primes are in the form of $6n + 1$ and $6n + 5$ consecutively. On December 2011, in [2], the largest known twin prime pair, $3756801695685 * 2^{666669} \pm 1$, were found with 200700 digits.

Similar to the distribution of prime numbers among positive integers, the number of twin primes less than N naturally declines as N increases. This brings up the question of how many pairs of twin primes are there?

Many research works have been devoted to provide a proof to the twin prime conjecture but it is still one of the open problems in mathematics and number theory. Some important result of twin primes and the gap between primes have been obtained. One of these results is Brun's constant (B). In 1919 Brun, [3],

proved that the sum of the reciprocals of the twin primes converge to a definite number called Brun's constant and has the value of $B = 1.90218 \pm 2 \cdot 10^{-5}$. The recently breakthrough, in 2013, of Yitang Zhang [5], where he proved that there are infinitely many pairs of primes with prime gap less than 70 million

$$\liminf_{n \rightarrow \infty} (p_{n+1} - p_n) < 7 \cdot 10^7.$$

This proof shows that the gap between primes does not grow infinitely, and it is bounded by a definite number. This result was significantly improved by several researchers.

In May 2013, mathematicians had uncovered simple tweaks to Zhang's argument that brought the bound below 60 million. A May 30 blog post by Scott Morrison of the Australian National University in Canberra ignited a firestorm of activity, as mathematicians vied to improve on this number, setting one record after another. By June 4, Terence Tao of the University of California, Los Angeles, a winner of the Fields Medal, mathematics' highest honor, had created a Polymath project, an open, online collaboration to improve the bound that attracted dozens of participants. For weeks, the project moved forward at a breathless pace. At times, the bound was going down every thirty minutes, Tao recalled. By July 27, the team had succeeded in reducing the proven bound on prime gaps from 70 million to 4,680.

On November 19 by James Maynard [4], a postdoctoral researcher working on his own at the University of Montreal, has upped the ante. Just months after Zhang announced his result, Maynard has presented an independent proof that pushes the gap down to 600. A new Polymath project is in the planning stages, to try to combine the collaboration's techniques with Maynard's approach to push this bound even lower, for more details please visit the website WIRED, Nov. 2013.

Strong connection between the twin prime and Goldbach's Conjectures was found along of our approach to prove the twin prime's conjecture. The Goldbach conjecture, dating from Goldbach's correspondence with Euler in 1742, that states: Every even integer greater than 2 is the sum of two prime numbers (not necessarily distinct). It has been verified that the even integers through 10^8 have the stated property, but Goldbach's conjecture remains unproved.

Several works on background information about Goldbach's conjecture have been conducted previously. Namely Dickson [6] lists results obtained through the first decade of this century. Wang, [7], is a collection of this century's most important papers on the Goldbach conjecture through the early 1980's. Shanks, [8], is a marvelous book on conjectures in number theory, Goldbach's among them, and on mathematical conjectures in general. Ribenboim, [9], is another treasure chest in number theory, with a section on Goldbach (pp. 229-235).

2 Abbreviation and Notation

Before starting the proof, some important definitions are needed to be introduced as it is indicated below

- Let p_2, \dots, p_n distinct ordered prime numbers, and for only notation reason we put $p_1 = 1$.
- For any two sets U and V of integer numbers, their sum and their difference is defined as follows

$$U \pm V = \{x \pm y : x \in U, y \in V\}.$$

- For any set U is multiplied by a value c is defined as follows

$$cU = \{c.x : x \in U\}.$$

- The difference between all elements of the set U , is noted by

$$\Delta U = \{x - y : (x, y) \in U^2\}.$$

- The set U/V is set of elements in U but not in V .
- The arithmetic sequence, with reason r , will be noted by $[r_0 : r : r_f]$, where r_0 and r_f are the initial and the final values of the sequence respectively, i.e.,

$$[r_0 : r : r_f] = \{r_0, r_0 + r, r_0 + 2r, \dots, r_f\}.$$

- If the the reason of the arithmetic sequence is equal to one then it will be noted simply by $[r_0 : r_f]$, i.e.,

$$[r_0 : r_f] = \{r_0, r_0 + 1, r_0 + 2, \dots, r_f\}.$$

- The function $\lfloor x \rfloor$ gives the largest integer less than or equal to x .
- The modulo operation is computing the remainder after division, m Modulo n will be noted as $m_{mod(n)}$, i.e.,

$$m_{mod(n)} = m - n \left\lfloor \frac{m}{n} \right\rfloor.$$

- The set V_x contains all co-prime numbers with all devisors of the integer x and are less than x .
- The set $V_{\prod_{i=1}^n p_i}$ contains all co-prime numbers with primes $p_i, i = \{1, 2, \dots, n\}$, and less than $\prod_{i=1}^n p_i$.
- The set w_k is the set of co-primes with primes $p_i, i = \{n - k + 2, \dots, n + 1\}$, and less then $\prod_{i=n-k+2}^{n+1} p_i$.

- Let $\pi(x)$ be the prime-counting function that gives the number of primes less or equal to x .
- Let $\pi(x, n)$ be the co-prime-counting function that gives the number of co-primes with $p_i, i > n$, and are less or equal to x .
- Let $\Psi(x, y, Q)$ be the number of all positive integers less than x which do not have a prime divisor which is less than y and belongs to Q .
- $U_{\prod_{i=1}^{n+1} p_i}^k = V_{\prod_{i=1}^{n+1} p_i} \cap \left[0 : \prod_{i=1}^{n+1-k} p_i\right]$, unless it is defined differently.
- $U_{\prod_{i=1}^{n+1} p_i}^{k,j} = V_{\prod_{i=1}^{n+1} p_i} \cap \left[j \prod_{i=1}^{n+1-k} p_i : (j+1) \prod_{i=1}^{n+1-k} p_i\right]$.
- The cardinality of a set U is noted by $Card(U)$.
- If the asymptomatic ration of two functions verify

$$\lim_{n \rightarrow \infty} \left| \frac{f(n)}{g(n)} \right| = 1,$$

then it will be noted by

$$f \sim g.$$

- If there exist positive δ and M such that

$$|f(x)| \leq M |g(x)| \quad \text{for } x > \delta,$$

then we write

$$f(x) = O(g(x)) \quad \text{as } x \rightarrow \infty.$$

- The greatest common divisor pf two integers, n and m, will be noted by

$$gcd(n, m).$$

3 Sketch of the proof

This section will summarized all the headlines of our approach, from the starting point, through important properties, till reaching the two conjectures. All headlines are briefed as follows

- Any odd number n can be written under the form of $n = 2k + 1$, where $k \in \mathbb{N}$.
- All co-primes numbers with 2 and 3 can be written under the form $6k + 1$ or $6k + 5$, so the two forms can be merged under one form $n = 6k + V_{2*3}$, where $k \in \mathbb{N}$ and the set $V_{2*3} = \{1, 5\}$.
- All co-primes number with 2, 3, and 5 can be written under the form of $n = 30k + V_{2*3*5}$, where $k \in \mathbb{N}$ and $V_{2*3*5} = \{1, 7, 11, 13, 17, 19, 23, 29\}$.

- Theorem 3.1 generalizes this idea of finding the shape of all co-primes number with $p_i, i \leq n+1$, as

$$n = k \left(\prod_{i=1}^{n+1} p_i \right) + V_{\text{mod}(\prod_{i=1}^{n+1} p_i)},$$

where the sets V are generated by the following recurrence formula

$$V_{\text{mod}(\prod_{i=1}^{n+1} p_i)} = \left(P_{n+1} V_{\text{mod}(\prod_{i=1}^n p_i)} + \left(\prod_{i=1}^n p_i \right) [1 : P_{n+1} - 1] \right)_{\text{mod}(\prod_{i=1}^{n+1} p_i)}.$$

- We have noticed and proved that for all $n \geq 2$

$$(V_{\prod_{i=1}^n p_i} - V_{\prod_{i=1}^n p_i})_{\text{mod}(\prod_{i=1}^n p_i)} = \left[0 : 2 : \prod_{i=1}^n p_i - 2 \right].$$

- We have noticed also that $\forall n \in \mathbb{N}$

$$\begin{aligned} V_{\prod_{i=1}^n p_i} &= \left\{ 1, p_{n+1}, \dots, \left(\prod_{i=1}^n p_i \right) - p_{n+1}, \left(\prod_{i=1}^n p_i \right) - 1 \right\} \\ \min V_{\prod_{i=1}^n p_i} / \{1\} &= p_{n+1} \\ V_{\prod_{i=1}^n p_i} \cap (1 : p_{n+1}) &= \emptyset. \end{aligned}$$

- The set $V_{\prod_{i=1}^n p_i} \cap (0 : p_{n+1}^2)$ contains only primes numbers.
- The asymptotic density of co-primes are found to be as follows

$$\begin{aligned} \pi(x, n) &\sim \ln(n) \frac{x}{\ln(x)}, \\ \frac{\pi(x, n)}{x} &\sim \frac{\ln(n)}{\ln(x)}, \\ &\text{and} \\ \frac{\text{card}(V_{\prod_{i=1}^n p_i})}{\prod_{i=1}^n p_i} &= \frac{\prod_{i=1}^n (p_i - 1)}{\prod_{i=1}^n p_i} \\ &\sim \exp \left(\int^n \frac{-dn}{n \ln(n)} \right) \\ &\sim \frac{C}{\ln(n)} \\ &\sim C \frac{\pi(n)}{n}. \end{aligned}$$

- In order to investigate the difference between only primes number, the primes inside the $V_{\prod_{i=1}^n p_i}$ will be considered as it is indicated in Lemma

3.5, which it gives extremely important properties as follows:

$$\left(\Delta V_{\prod_{i=1}^{n+1} p_i}\right)_{\text{mod}(\prod_{i=1}^{n+1} p_i)} = \left(\Delta U_{\prod_{i=1}^{n+1} p_i}^k\right)_{\text{mod}(\prod_{i=1}^{n+1-k} p_i)} + \sum_{j=0}^{k-1} \left(\prod_{i=1}^{n-j} p_i\right) [0 : p_{n+1-j}-1],$$

and

$$\Delta U_{\prod_{i=1}^{n+1} p_i}^{k,j} \supseteq \left(\Delta V_{\prod_{i=1}^{n+1-k} p_i}\right)_{\text{mod}(\prod_{i=1}^{n+1-k} p_i)} = [0 : 2 : \prod_{i=1}^{n-k} p_i - 2],$$

where $j \leq \prod_{i=n-k+2}^{n+1} p_i$.

- We can choose the integer k such that all elements inside of $U_{\prod_{i=1}^{n+1} p_i}^k$ are primes. Since the range of set is large and

$$\begin{aligned} \lim_{k \rightarrow \infty} \min_k U_{\prod_{i=1}^{n+1} p_i}^{k,j} / \{1\} &= +\infty \\ \lim_{k \rightarrow \infty} \max_k U_{\prod_{i=1}^{n+1} p_i}^{k,j} / \{1\} &= +\infty, \end{aligned}$$

and

$$\Delta U_{\prod_{i=1}^{n+1} p_i}^{k,j} = [0 : 2 : \prod_{i=1}^{n-k} p_i - 2],$$

it leads to the infinity existence of twin prime number and to the fact that every even integer greater than 2 can be expressed as the difference of two primes

$$\liminf_{n \rightarrow \infty} (p_n - p_{n+1}) = 2.$$

- Since there is no prime between two primes that defer by 4, we can conclude the existence of infinitely many cousin primes, $p_{n+1} - p_n = 4$, i.e.,

$$\lim_{n \rightarrow \infty} \sum_{k > n} 1_{\{p_k - p_{k+1} = 4\}} \neq 0.$$

- we can prove that if every even integer greater than 2 can be expressed as the difference of two primes then every even integer greater than 2 can be expressed as the sum of two primes.
- Other methods are highlighted during the proofs.

The initial idea of these above points comes from the way of generating sets of co-prime numbers recursively by adding one prime at each step as it is indicated by the following theorem

Theorem 3.1. *Any co-prime number, n , with the first m prime numbers can be expressed according to the following equation*

$$n = \left(\prod_{i=1}^m P_i \right) k + l,$$

where $k \in \mathbb{Z}$, and $l \in V_{\text{mod}(\prod_{i=1}^m P_i)}$ a set of co-prime numbers with the first $m-1$ prime numbers, p_2, \dots, p_m .

The set of co-prime numbers, $V_{\text{mod}(\prod_{i=1}^{m+1} P_i)}$, can be generated recursively as follows:

$$V_{\text{mod}(\prod_{i=1}^{m+1} P_i)} = \left(P_{m+1} V_{\text{mod}(\prod_{i=1}^m P_i)} + \left(\prod_{i=1}^m P_i \right) [1 : P_{m+1} - 1] \right)_{\text{mod}(\prod_{i=1}^{m+1} P_i)}.$$

Concluding that any number $x \in V_{\text{mod}(\prod_{i=1}^m P_i)} \cap (1 : p_{m+1}^2)$ is a prime number.

Some of important properties of set of co-prime numbers that will be very often used along this paper are highlighted by the following lemma

Lemma 3.2. *i. For all co-primes x and y , we have the following two properties:*

$$y = (x [1 : y - 1])_{\text{mod}(y)} = [1 : y - 1]_{\text{mod}(y)}$$

$$\forall z_1 \in [1 : y - 1], \exists! z_2 \in [1 : y - 1], z_2 \neq z_1, \text{ such that } z_1 = (z_2 x)_{\text{mod}(y)}$$

ii. If y is a co-prime number with P_i , $i \leq m$, we have the following properties:

$$V_{\text{mod}(\prod_{i=1}^m P_i)} = \left(y V_{\text{mod}(\prod_{i=1}^m P_i)} \right)_{\text{mod}(\prod_{i=1}^m P_i)}.$$

$$\forall z_1 \in V_{\text{mod}(\prod_{i=1}^m P_i)}, \exists! z_2 \in V_{\text{mod}(\prod_{i=1}^m P_i)}, z_2 \neq z_1, \text{ such that } z_1 = (z_2 x)_{\text{mod}(\prod_{i=1}^m P_i)}.$$

The main ideas of our proofs are on creating and on analysing of set sequence of distinct co-primes with the first n primes, $H = (x_1, \dots, x_k)$, by using Theorem 3.1 and the important properties of the linear combination of the co-prime sets, $H = \{1, p_{n+1}, \dots, \prod_{i=1}^n p_i - 1\}$, that give sets of even numbers $\{0, 2, 4, \dots, \prod_{i=1}^n p_i - 2\}$. The next three lemmas will explain our approach gradually.

First of all, some properties of the difference between sets of co-prime numbers will be pointed out and a recursive formula between these sets will be expressed as well.

Lemma 3.3. For all $n \geq 2$ and for all $k \geq 0$, we have the following equalities

1. The difference co-primes of the sets V , generate compact subsets of even numbers

$$\begin{aligned} (\Delta V_{\prod_{i=1}^n p_i})_{\text{mod}(\prod_{i=1}^n p_i)} &= (V_{\prod_{i=1}^n p_i} - V_{\prod_{i=1}^n p_i})_{\text{mod}(\prod_{i=1}^n p_i)} \\ &= \left[0 : 2 : \prod_{i=1}^n p_i - 2 \right]. \end{aligned}$$

2. $V_{\prod_{i=1}^{n+1} p_i} = \left(\left(\prod_{i=n-k+2}^{n+1} p_i \right) \left(V_{\prod_{i=1}^{n-k+1} p_i} \right) + w_k \left(\prod_{i=1}^{n-k+1} p_i \right) \right)_{\text{mod}(\prod_{i=1}^{n+1} p_i)}$, where the set w_k is the set of co-primes number with p_i , for $i \in \{n-k+2, \dots, n+1\}$.

The recursive relation between sets w , can be deducted, for $k > 1$, as follows

$$w_{k+1} = w_k p_{n-k+1} + \left(\prod_{i=n-k+2}^{n+1} p_i \right) [1 : p_{n-k+1} - 1].$$

As initial investigation inside the set V , a new question is raised about finding subsets that verified the first part of lemma 3.3, the next lemma gives interesting result

Lemma 3.4. For all n bigger than 1, let's define the following sets

$$U_{\prod_{i=1}^{n+1} p_i} = \left\{ x \in V_{\prod_{i=1}^{n+1} p_i} : x \in \left[0, 4 \prod_{i=1}^n p_i \right] \right\},$$

then

$$(\Delta U_{\prod_{i=1}^{n+1} p_i})_{\text{mod}(\prod_{i=1}^{n+1} p_i)} \supseteq (\Delta V_{\prod_{i=1}^n p_i})_{\text{mod}(\prod_{i=1}^n p_i)},$$

and

$$(\Delta U_{\prod_{i=1}^{n+1} p_i}) \supseteq \left[0 : 2 : \left(\prod_{i=1}^n p_i \right) - 2 \right]$$

In order to explain the idea on how to prove that the difference or summation between all prime numbers is equals to the set of all even integers, the following lemma, a generalization and improved version of lemma 3.4, will help us to limit the difference only between primes numbers.

Lemma 3.5. For all integer $n > 3$, it exists $k_0 \in \mathbb{N}$, such that for all integer $k < k_0$, the difference between co-primes numbers, V , can be expressed recursively in function of difference between subsets of V , as it is indicated below

$$(\Delta V_{\prod_{i=1}^{n+1} p_i})_{\text{mod}(\prod_{i=1}^{n+1} p_i)} = (\Delta U_{\prod_{i=1}^{n+1} p_i}^{k,j})_{\text{mod}(\prod_{i=1}^{n+1-k} p_i)} + \sum_{j=0}^{k-1} \left(\prod_{i=1}^{n-j} p_i \right) [0 : p_{n+1-j} - 1],$$

where $U_{\prod_{i=1}^{n+1} p_i}^{k,j} = V_{\prod_{i=1}^{n+1} p_i} \cap \left[j \prod_{i=1}^{n+1-k} p_i : (j+1) \prod_{i=1}^{n+1-k} p_i \right]$.

To extend this result and omit the modulo from the right side of the previous equation i.e., from the set $\Delta U_{\prod_{i=1}^{n+1-k} p_i}^k$, we enlarge the definition of the set as

$$U_{\prod_{i=1}^{n+1} p_i}^{k,j} = V_{\prod_{i=1}^{n+1} p_i} \cap \left[j \prod_{i=1}^{n+1-k} p_i : (j+2) \prod_{i=1}^{n+1-k} p_i \right],$$

then it leads, under the condition that $\prod_{i=1}^{k-2} p_i > p_{n+2}$ to

- $\Delta U_{\prod_{i=1}^{n+1} p_i}^k \supseteq \left(\Delta V_{\prod_{i=1}^{n+1-k} p_i} \right)_{\text{mod}(\prod_{i=1}^{n+1-k} p_i)} = [0 : 2 : \left(\prod_{i=1}^{n+1-k} p_i \right) - 2],$
- For all integers $j \leq \prod_{i=n+2-k}^{n+1} p_i$, we have

$$\Delta U_{\prod_{i=1}^{n+1} p_i}^{k,j} \supseteq \left(\Delta V_{\prod_{i=1}^{n+1-k} p_i} \right)_{\text{mod}(\prod_{i=1}^{n+1-k} p_i)} = [0 : 2 : \left(\prod_{i=1}^{n+1-k} p_i \right) - 2].$$

The threshold k_0 will be the smallest integer verified the condition, i.e.,

$$k_0 = \min \{k : \prod_{i=1}^{k-2} p_i > p_{n+2}\}.$$

An important result will be needed in order to prove the lemma 3.5, evaluation the density of co-primes with $p_i, i > n$, and are less or equal to x , noted $\pi(x, n)$. RiChard Warlimont, [10], and D. A. Golden, [11], have worked on the estimation of co-primes density under certain conditions, our following lemma will express an asymptotic density of co-primes with consecutive primes.

Lemma 3.6. Let Q be a set of primes and we denote by $\Psi(x, y, Q)$ the number of all positive integers less than x which do not have a prime divisor which is less than y and belongs to Q .

Put $P_Q := \prod_{p_i \in Q} p_i$, $y < \min_i \{p_i \mid p_i \in Q\}$, and let $R(y) = \frac{1}{\ln(y)}$.

Then we have the following statements

- (i) For any positive integers k we have

$$\Psi(x, y, Q) = \text{Card} \{i \in (y + kP_Q, x + kP_Q] \mid \gcd(i, P_Q) = 1\}.$$

- (ii) For any positive integers k we have

$$\Psi(x, y, Q) = \Psi(x + kP_Q, y, Q) - \Psi(y + kP_Q, y, Q) + y,$$

and if $x < P_Q$ and $\gcd(x, P_Q) = 1$ then

$$\Psi(x, y, Q) + \Psi(P_Q - x, y, Q) = \Psi(P_Q, y, Q) + 1 = P_Q \prod_{p_i \in Q} \left(1 - \frac{1}{p_i}\right) + 1.$$

(iii) Uniformly in $1.5 \leq y \leq x$ we have

$$\Psi(x, y, Q) = (x - y) \prod_{p_i \in Q} \left(1 - \frac{1}{p_i}\right) (1 + O(R(y))) + y.$$

(iv) If x and y are big enough and $Q = \{p_i \mid y < p_i \leq x\}$ then

$$\Psi(x, y, Q) \sim (x - y) \frac{\ln(y)}{\ln(x)} + y,$$

and if $y/x \rightarrow 0$ then

$$\Psi(x, y, Q) \sim \pi(x, y/\ln(y)) \sim x \frac{\ln(y)}{\ln(x)}.$$

The coming sections will be devoted to prove the Theorem 3.1 and the Lemma 3.2 at first step of our approach as an introduction to the proof of the lemma 3.3, 3.4, and 3.5 respectively.

Finally the proof of the two conjectures with their extension will be at the end of this paper.

4 Proof of Theorem 3.1

Let n and b be two positive integers. If n is not divisible by a , then a needs to be a multiple of k added to another positive integer b , where b is smaller than a ; under the condition that a and b are co-primes, the positive integer n is co-prime with a . This idea leads to the generation of a large prime number from a sequence of previous prime numbers. This idea can be written in mathematical form as follows:

$$n = ak + b, \text{ where } b < a,$$

if a and b are co-primes then a and n are also co-prime numbers.

We will generalize this idea to generate co-prime numbers recursively by including one prime at each step.

Let $\omega(m)$ be a set of co-primes with the first m prime numbers, so ω can be expressed as:

$$\omega(m) = \left(\prod_{i=1}^m p_i \right) . k + V_{\text{mod}(\prod_{i=1}^m p_i)},$$

A recursive question will be raised in how to find the set $V_{\text{mod}(\prod_{i=1}^{m+1} p_i)}$ from the $V_{\text{mod}(\prod_{i=1}^m p_i)}$ in order to extract all elements of $\omega(m+1)$. To do that, let suppose $\omega(m)$ is co-prime also with (p_{m+1}) and by definition it is co-prime with $(\prod_{i=1}^m p_i)$, so it exists two integers, k and k' such that

$$\begin{cases} \omega(m+1) = (\prod_{i=1}^m p_i).k + V_{mod}(\prod_{i=1}^m p_i) \\ \omega(m+1) = (p_{m+1}).k' + [1 : (p_{m+1} - 1)], \end{cases} \quad (1)$$

Let suppose the integer x_1 as a co-prime with all p_i , $i \leq m$, and x_2 is co-prime with p_{m+1} , by using Lemma 3.2 the previous system of equations can be formulated as follows:

$$\begin{cases} \omega(m+1) = (\prod_{i=1}^m p_i).k + V_{mod}(\prod_{i=1}^m p_i)x_1 \\ \omega(m+1) = (p_{m+1}).k' + [1 : (p_{m+1} - 1)]x_2, \end{cases} \quad (2)$$

Without losing generality let $x_1 = p_{m+1}$ and $x_2 = \prod_{i=1}^m p_i$ so $\omega(m+1)$ can be expressed by

$$\begin{cases} \omega(m+1) = (\prod_{i=1}^m p_i).k + V_{mod}(\prod_{i=1}^m p_i)p_{m+1} \\ \omega(m+1) = (p_{m+1}).k' + [1 : (p_{m+1} - 1)] \prod_{i=1}^m p_i, \end{cases} \quad (3)$$

The set of co-primes can be expressed as given below:

$$\left(\prod_{i=1}^m p_i \right).k - (p_{m+1}).k' = [1 : (p_{m+1} - 1)] \prod_{i=1}^m p_i - V_{mod}(\prod_{i=1}^m p_i)p_{m+1} \quad (4)$$

Let $l_1 \in [1 : (p_{m+1} - 1)]$ and $l_2 \in V_{mod}(\prod_{i=1}^m p_i)$.

To calculate $\omega(m+1)$ the equation 4 needs to be solved, by subtraction their two equations we can find

$$\prod_{i=1}^m p_i \cdot (k - l_1) = (p_{m+1}) \cdot (k' - l_2),$$

where $(k - l_1)$ and $(k' - l_2)$ can be calculated as:

$$\begin{cases} (k - l_1) = \vartheta.p_{m+1} \\ (k' - l_2) = \vartheta.(\prod_{i=1}^m p_i), \end{cases}$$

where ϑ is any value inside Z .

By isolating the two variables k and k' , we have:

$$\begin{cases} k = \vartheta.p_{m+1} + l_1. \\ k' = \vartheta.(\prod_{i=1}^m p_i) + l_2, \end{cases}$$

Substituting the value of k in system (3), we have:

$$\begin{cases} \omega(m+1) = \vartheta \left(\prod_{i=1}^{m+1} p_i \right) + l_1 (\prod_{i=1}^m p_i) + V_{mod}(\prod_{i=1}^m p_i) \\ \omega(m+1) = \vartheta \left(\prod_{i=1}^{m+1} p_i \right) + l_2 (p_{m+1}) + [1 : (p_{m+1} - 1)], \end{cases}$$

By substitution the values of l_1 and l_2 in the above equations we conclude

$$\begin{cases} \omega(m+1) = \vartheta. \left(\prod_{i=1}^{m+1} p_i \right) + ([1 : (p_{m+1} - 1)] \cdot (\prod_{i=1}^m p_i)) + (p_{m+1}) \cdot V_{mod(\prod_{i=1}^m p_i)} \\ \omega(m+1) = \vartheta. \left(\prod_{i=1}^{m+1} p_i \right) + ([1 : (p_{m+1} - 1)] \cdot (\prod_{i=1}^m p_i)) + (p_{m+1}) \cdot V_{mod(\prod_{i=1}^m p_i)}, \end{cases}$$

where both equations are equivalent due to the similarity of property of the modulo of the last term.

The general formula of $\omega(m+1)$ that are co-primes with the first $m+1$ prime numbers will be as follows:

$$\omega(m+1) = \vartheta. \left(\prod_{i=1}^{m+1} p_i \right) + \left([1 : (p_{m+1} - 1)] \cdot \left(\prod_{i=1}^m p_i \right) \right) + (p_{m+1}) \cdot V_{mod(\prod_{i=1}^m p_i)},$$

We can general also the set of co-primes with the first $m+1$ prime numbers in order to get the following:

$$\omega(m+1) = \vartheta. \left(\prod_{i=1}^{m+1} p_i \right) + V_{mod(\prod_{i=1}^{m+1} p_i)},$$

where

$$V_{mod(\prod_{i=1}^{m+1} p_i)} = \left([1 : (p_{m+1} - 1)] \cdot \left(\prod_{i=1}^m p_i \right) + (p_{m+1}) \cdot V_{mod(\prod_{i=1}^m p_i)} \right)_{mod(\prod_{i=1}^{m+1} p_i)}.$$

■

5 Proof of Lemma 3.2

5.1 Proof of Lemma 3.2 part (i)

We will start proving the first part of the Lemma 3.2 with following equality:

$$\left(\prod_{i=1}^m p_i \right) \cdot [1 : (p_{m+1} - 1)]_{mod(p_{m+1})} = [1 : (p_{m+1} - 1)]_{mod(p_{m+1})}.$$

Since $(\prod_{i=1}^m p_i)$ is co-prime with p_{m+1} , there exists $k \in \mathbb{N}$, where $(\prod_{i=1}^m p_i)$ can be written as:

$$(\prod_{i=1}^m p_i) = k \cdot p_{m+1} + r, \text{ where } 1 \leq r < p_{m+1}.$$

Then it implies that

$$(k \cdot p_{m+1} + r) [1, 2, 3, \dots, (p_{m+1} - 1)]_{p_{m+1}} = [r, 2r, 3r, \dots, (p_{m+1} - 1) \cdot r]_{p_{m+1}}.$$

By contradiction we can prove that

$$[ir]_{\text{mod}(p_{m+1})} \neq 0 \quad (5)$$

If $[ir]_{\text{mod}(p_{m+1})} = 0$, then it exists $\mu \in \mathbb{Z}$ such that $ir = \mu p_{m+1}$, which it means that i or r are multiple of p_{m+1} , where it contradicts of the fact that i and r are both less than p_{m+1} .

To finish the proof of Lemma 3.2 part (i) and first part of (ii), we still need to show by contraction the following:

$$[ir]_{\text{mod}(p_{m+1})} = [jr]_{\text{mod}(p_{m+1})}, \quad \forall i \neq j \in \{1, 2, \dots, p_{m+1} - 1\} \quad (6)$$

Let's suppose that it exists two integers i and j such that:

$$\begin{cases} ir = k' \cdot p_{m+1} + r_0, & k' \in \mathbb{Z} \\ jr = k'' \cdot p_{m+1} + r_0, & k'' \in \mathbb{Z} \end{cases}$$

By subtracting the two equation, we have that

$$(i - j)r = (k' - k'') \cdot p_{m+1},$$

which it contradicts with the equation 5 due to the facts that

$$\begin{aligned} r &\in [1 : p_{m+1} - 1] \\ (i - j)_{\text{mod}(p_{m+1})} &\leq p_{m+1} - 1 \end{aligned}$$

From the equations 5 and 6, The following equation can be deducted easily

$$[r \ 2r \ 3r \ \dots \ (p_{m+1} - 1)r]_{\text{mod}(p_{m+1})} = [1 : (p_{m+1} - 1)]_{\text{mod}(p_{m+1})},$$

then it implies that

$$\left(\prod_{i=1}^m p_i \right) \cdot [1 : (p_{m+1} - 1)]_{\text{mod}(p_{m+1})} = [1 : (p_{m+1} - 1)]_{\text{mod}(p_{m+1})}.$$

Since for all all two co-primes, k_1 and k_2 , we can write $(k_1)_m \text{od}(k_2) = r$, where $r \in [1 : k_2]$, then we can Generalize our result as follows

$$(k_1 [1 : (k_2 - 1)])_{\text{mod}(k_2)} = [1 : (k_2 - 1)]_{\text{mod}(k_2)}.$$

■

5.2 Proof of Lemma 3.2 part (ii)

Here we will prove the second part of Lemma 3.2

$$p_{m+1} \cdot V_{\text{mod}(\prod_{i=1}^m p_i)} = V_{\text{mod}(\prod_{i=1}^m p_i)},$$

For all $m > 1$; the cardinality of the set V can be calculated as follows

$$\text{Card}\left(V_{\text{mod}(\prod_{i=1}^m p_i)}\right) = \prod_{i=2}^m (p_i - 1).$$

Let $\text{Card}\left(V_{\text{mod}(\prod_{i=1}^m p_i)}\right) = M$, so

$$V_{\text{mod}(\prod_{i=1}^m p_i)} = \{r_1, r_2, r_3, \dots, r_M\}.$$

Now, we will test first the non existing of $i \in \{1, 2, \dots, M\}$ such that:

$$r_i : r_i p_{m+1} = k \left(\prod_{i=1}^m p_i \right),$$

if the last equation is true, then for all $j \leq m$ we have

$$\frac{r_i}{p_j} \in \mathbb{N},$$

which it implies that

$$r_i = k' \left(\prod_{i=1}^m p_i \right),$$

this statement contradict with the fact that $r_i \in V_{\text{mod}(\prod_{i=1}^m p_i)}$, i.e.,

$$(r_i)_{\text{mod}(\prod_{i=1}^m p_i)} \neq 0.$$

To complete the proof, second test needs to be checked :

$$\exists i \neq j \text{ such that } [(r_i) p_{m+1}]_{\text{mod}(\prod_{i=1}^m p_i)} = [(r_j) p_{m+1}]_{\text{mod}(\prod_{i=1}^m p_i)},$$

which it implies that r_i and r_j have the following values:

$$\begin{cases} r_i p_{m+1} = k' \left(\prod_{i=1}^m p_i \right) + r_0 & k' \in \mathbb{Z} \\ r_j p_{m+1} = k'' \left(\prod_{i=1}^m p_i \right) + r_0 & k'' \in \mathbb{Z} \end{cases},$$

where $r_0 \in [1 : \prod_{i=1}^m p_i - 1]$.

By subtracting the above two equations, we can get

$$(r_i - r_j) p_{m+1} = \left(\prod_{i=1}^m p_i \right) (k' - k''),$$

which it means that $(r_i - r_j)$ has p_1, p_2, \dots, p_m as divisors, so as consequence we can write

$$(r_i - r_j) \geq \left(\prod_{i=1}^m p_i \right),$$

again this statement contradict with the fact that the integers r_i are less than $\prod_{i=1}^m p_i$.

We can conclude now

$$\forall i \neq j, [(r_i) p_{m+1}]_{\text{mod}(\prod_{i=1}^m p_i)} \neq [(r_j) p_{m+1}]_{\text{mod}(\prod_{i=1}^m p_i)}.$$

The lemma 3.2 (ii), part two, can be concluded since the cardinality of the set $V_{(\prod_{i=1}^m p_i)}$ is preserved after multiplying it by a co-prime integer.

■

6 Proof of Lemma 3.3

6.1 Proof of Lemma 3.3 part (i)

The proof by induction will be used to prove the first part. The case where $n = 2$ is trivial to be checked, $1-1=0$. For $n = 3$ the co-prime set with the two primes 2 and 3 is defined by $V_{\prod_{i=1}^3 p_i} = \{1, 5\}$, then

$$\Delta V_{\prod_{i=1}^3 p_i} = \{1, 5\} - \{1, 5\} = \{0, 4, -4\}$$

which implies that

$$\left(\Delta V_{\prod_{i=1}^3 p_i} \right)_{\text{mod}(\prod_{i=1}^3 p_i)} = \{0, 2, 4\}_{\text{mod}(\prod_{i=1}^3 p_i)}.$$

Let's assume that the formula is correct for n and we need to prove the formula for $n+1$. From the assumption that $(\Delta V_{\prod_{i=1}^n p_i})_{\text{mod}(\prod_{i=1}^n p_i)} = [0 : 2 : \prod_{i=1}^n p_i - 2]$, the next formula needs to be concluded,

$$\left(\Delta V_{\prod_{i=1}^{n+1} p_i} \right)_{\text{mod}(\prod_{i=1}^{n+1} p_i)} = \left[0 : 2 : \prod_{i=1}^{n+1} p_i - 2 \right].$$

Note that, from Lemma 3.2, that

$$(p_{n+1} V_{\prod_{i=1}^n p_i})_{\text{mod}(\prod_{i=1}^n p_i)} = V_{\prod_{i=1}^n p_i}.$$

then

$$(p_{n+1} \Delta V_{\prod_{i=1}^n p_i})_{\text{mod}(\prod_{i=1}^n p_i)} = (\Delta V_{\prod_{i=1}^n p_i})_{\text{mod}(\prod_{i=1}^n p_i)}.$$

Further, from theorem 3.1, we have that

$$\Delta V_{\prod_{i=1}^{n+1} p_i} = \left(p_{n+1} V_{\prod_{i=1}^n p_i} + \prod_{i=1}^n p_i [1 : p_{n+1} - 1] \right) - \left(p_{n+1} V_{\prod_{i=1}^n p_i} + \prod_{i=1}^n p_i [1 : p_{n+1} - 1] \right)$$

this difference gives

$$(\Delta V_{\prod_{i=1}^{n+1} p_i})_{\text{mod}(\prod_{i=1}^{n+1} p_i)} = \left(p_{n+1} \Delta V_{\prod_{i=1}^n p_i} + \prod_{i=1}^n p_i [2 - p_{n+1} : p_{n+1} - 2] \right)_{\text{mod}(\prod_{i=1}^{n+1} p_i)}.$$

And from lemma 3.2, we have

$$\left(p_{n+1} \left[1 : 1 : \prod_{i=3}^n p_i - 1 \right] \right)_{\text{mod}(\prod_{i=3}^n p_i)} = \left[1 : 1 : \prod_{i=3}^n p_i - 1 \right]$$

by multiplying the previous equation by 2 and including a value zero to the both side, it leads to

$$0 \cup \left(2p_{n+1} \left[1 : 1 : \prod_{i=3}^n p_i - 1 \right] \right)_{\text{mod}(\prod_{i=3}^n p_i)} = 0 \cup 2 \left[1 : 1 : \prod_{i=3}^n p_i - 1 \right]$$

which it can be rewritten as follows

$$\left(p_{n+1} \left[0 : 2 : \prod_{i=1}^n p_i - 2 \right] \right)_{\text{mod}(\prod_{i=1}^n p_i)} = \left[0 : 2 : \prod_{i=1}^n p_i - 2 \right].$$

By combining these properties leads to

$$\begin{aligned} (\Delta V_{\prod_{i=1}^{n+1} p_i})_{\text{mod}(\prod_{i=1}^{n+1} p_i)} &= \left(p_{n+1} \left[0 : 2 : \prod_{i=1}^n p_i - 2 \right] + \left(\prod_{i=1}^n p_i \right) [2 - p_{n+1} : p_{n+1} - 2] \right)_{\text{mod}(\prod_{i=1}^{n+1} p_i)} \\ &= \left(\left[0 : 2 : \prod_{i=1}^n p_i - 2 \right] + \left(\prod_{i=1}^n p_i \right) [2 - p_{n+1} : p_{n+1} - 2] \right)_{\text{mod}(\prod_{i=1}^{n+1} p_i)}. \end{aligned}$$

The key idea of this lemma comes from previous equation, which it can be derived differently as the following

For all $i \in [0 : 2 : \prod_{i=1}^n p_i - 2]$, $\exists l_0 < p_{n+1}$ such that

$$i + l_0 \prod_{i=1}^n p_i \in p_{n+1} \left[0 : 2 : \prod_{i=1}^n p_i - 2 \right],$$

this yields

$$\left(\Delta V_{\prod_{i=1}^{n+1} p_i}\right)_{\text{mod}(\prod_{i=1}^{n+1} p_i)} = \left(\bigcup_{i \in [0:2:\prod_{i=1}^n p_i - 2]} \left\{ i + l_0 \prod_{i=1}^n p_i \right\} + \left(\prod_{i=1}^n p_i\right) [2 - p_{n+1} : p_{n+1} - 2] \right)_{\text{mod}(\prod_{i=1}^{n+1} p_i)}.$$

Since

$$\left(l_0 \prod_{i=1}^n p_i + \left(\prod_{i=1}^n p_i\right) [2 - p_{n+1} : p_{n+1} - 2]\right)_{\text{mod}(\prod_{i=1}^{n+1} p_i)} = \left(\left(\prod_{i=1}^n p_i\right) [2 - p_{n+1} : p_{n+1} - 2]\right)_{\text{mod}(\prod_{i=1}^{n+1} p_i)}$$

which it leads to

$$\left(\Delta V_{\prod_{i=1}^{n+1} p_i}\right)_{\text{mod}(\prod_{i=1}^{n+1} p_i)} = \left(\bigcup_{i \in [0:2:\prod_{i=1}^n p_i - 2]} \{i\} + \left(\prod_{i=1}^n p_i\right) [2 - p_{n+1} : p_{n+1} - 2]\right)_{\text{mod}(\prod_{i=1}^{n+1} p_i)}$$

and

$$\left(\Delta V_{\prod_{i=1}^{n+1} p_i}\right)_{\text{mod}(\prod_{i=1}^{n+1} p_i)} = \left(\left[0 : 2 : \prod_{i=1}^n p_i - 2\right] + \left(\prod_{i=1}^n p_i\right) [2 - p_{n+1} : p_{n+1} - 2]\right)_{\text{mod}(\prod_{i=1}^{n+1} p_i)}.$$

Finally, from the last equation, it follows that

$$\left(\Delta V_{\prod_{i=1}^{n+1} p_i}\right)_{\text{mod}(\prod_{i=1}^{n+1} p_i)} = \left[0 : 2 : \prod_{i=1}^{n+1} p_i - 2\right].$$

■

6.2 Proof of Lemma 3.3 part (ii)

From the recursive formula of Theorem 3.1, we have the following

$$\begin{aligned} V_{\prod_{i=1}^{n+1} p_i} &= \left(p_{n+1} V_{\prod_{i=1}^n p_i} + \prod_{i=1}^n p_i [1 : p_{n+1} - 1]\right)_{\text{mod}(\prod_{i=1}^{n+1} p_i)} \\ &= p_{n+1} \left(p_n V_{\prod_{i=1}^{n-1} p_i} + \prod_{i=1}^{n-1} p_i [1 : p_n - 1]\right) + \left(\prod_{i=1}^n p_i\right) [1 : p_{n+1} - 1] \\ &= p_{n+1} p_n V_{\prod_{i=1}^{n-1} p_i} + p_{n+1} \prod_{i=1}^{n-1} p_i [1 : p_n - 1] + \prod_{i=1}^n p_i [1 : p_{n+1} - 1] \\ &= p_{n+1} p_n V_{\prod_{i=1}^{n-1} p_i} + \prod_{i=1}^{n-1} p_i (p_{n+1} [1 : p_n - 1] + p_n [1 : p_{n+1} - 1]) \end{aligned}$$

Further, the set $V_{\prod_{i=1}^{n+1} p_i}$ can be written in term of $V_{\prod_{i=1}^{n-1} p_i}$ as follows

$$V_{\prod_{i=1}^{n+1} p_i} = \left(p_{n+1} p_n V_{\prod_{i=1}^{n-1} p_i} + \left(\prod_{i=1}^{n-1} p_i \right) (w_2) \right)_{\text{mod}(\prod_{i=1}^{n+1} p_i)},$$

where $w_2 = (p_{n+1}[1 : p_n - 1] + p_n[1 : p_{n+1} - 1])$. We can go further by generating general sequence in terms of w_i as follows

$$V_{\prod_{i=1}^{n+1} p_i} = \left(\prod_{i=n-k+2}^{n+1} p_i \right) (V_{\prod_{i=1}^{n-k+1} p_i}) + w_k \left(\prod_{i=1}^{n-k+1} p_i \right),$$

the last equation leads to

$$V_{\prod_{i=1}^{n+1} p_i} = \prod_{i=n-k+2}^{n+1} p_i \left(p_{n-k+1} (V_{\prod_{i=1}^{n-k} p_i}) + \left(\prod_{i=1}^{n-k} p_i \right) [1 : p_{n-k+1} - 1] \right) + w_k \prod_{i=1}^{n-k+1} p_i,$$

then the general term of the sequence, w_k , can be obtained from w_k as recursive formula

$$w_{k+1} \prod_{i=1}^{n-k} p_i = w_k \prod_{i=1}^{n-k+1} p_i + \left(\prod_{i=1}^{n-k} p_i \right) \left(\prod_{i=n-k+2}^{n+1} p_i \right) [1 : p_{n-k+1} - 1], \quad \forall k \geq 1,$$

Then

$$w_{k+1} = w_k p_{n-k+1} + \left(\prod_{i=n-k+2}^{n+1} p_i \right) [1 : p_{n-k+1} - 1].$$

It still remains to prove that w_k is the set of co-primes with p_i , where $i = \{n - k + 2, \dots, n + 1\}$. Let's start by w_2 since w_1 is obvious.

By definition $V_{p_{n+1} p_n}$ is a set of all co-prime number with p_{n+1} and p_n and bounded by $p_{n+1} p_n$ and also V_{p_n} and $V_{p_{n+1}}$ be co-primes number with p_n and p_{n+1} respectively, then

$$\begin{cases} V_{p_n} = k p_n + [1 : p_n - 1], & k \in \mathbb{Z} \\ V_{p_{n+1}} = k' p_{n+1} + [1 : p_{n+1} - 1] & k' \in \mathbb{Z}, \end{cases} \quad (7)$$

and From Lemma 3.2, in mod p_n equation, we have

$$\begin{cases} V_{p_n} = k p_n + p_{n+1} [1 : p_n - 1] \\ V_{p_{n+1}} = k' p_{n+1} + p_n [1 : p_{n+1} - 1] \end{cases} \quad (8)$$

To get the form of co-primes with p_n and p_{n+1} , $V_{p_n} \cap V_{p_{n+1}}$, then by Subtracting both equations we get

$$k' p_{n+1} - k p_n = p_{n+1} [1 : p_n - 1] - p_n [1 : p_{n+1} - 1],$$

Since $p_{n+1}[1 : p_n - 1] - p_n[1 : p_{n+1} - 1]$ is co-primes with p_n and p_{n+1} , then it exists particular solution k_0 and k'_0 , that leads to general solution

$$\begin{cases} k = k_0 + hp_{n+1} \\ k' = k'_0 + hp_n, \end{cases} \quad (9)$$

where h is any integer.

Hence, V_{p_n} can be written under the following form

$$V_{p_n} \cap V_{p_{n+1}} = p_{n+1}p_n h + p_n k_0 + [1 : p_n - 1],$$

where $k_0 = k'_0 p_n + p_{n+1}[1 : p_n - 1] - p_n[1 : p_{n+1} - 1]$, then

$$V_{p_n} \cap V_{p_{n+1}} = p_{n+1}p_n(h + k'_0) + p_n[1 : p_{n+1} - 1] - p_{n+1}[1 : p_n - 1].$$

Since p_{n+1} and p_n are co-primes and by using the property of mod from lemma 1, then $(p_{n+1}p_n - p_{n+1}[1 : p_n - 1])_{\text{mod}(p_{n+1}p_n)} = (p_{n+1}[1 : p_n - 1])_{\text{mod}(p_{n+1}p_n)}$, The set $V_{p_{n+1}p_n}$, co-prime numbers with $p_{n+1}p_n$, can be defined as follows:

$$\begin{aligned} V_{p_{n+1}p_n} &= V_{p_n} \cap V_{p_{n+1}} \\ &= (p_n[1 : p_{n+1} - 1] - p_{n+1}[1 : p_n - 1])_{\text{mod}(p_{n+1}p_n)} \\ &= (p_n[1 : p_{n+1} - 1] + p_{n+1}[1 : p_n - 1])_{\text{mod}(p_{n+1}p_n)}, \end{aligned}$$

then $w_k = V_{p_{n+1}p_n}$.

We can prove easily that w_{k+1} is co-primes with p_i , where $i = \{n - k + 1, n - k + 2, \dots, n + 1\}$ under the assumption that w_k is co-primes with p_i , where $i = \{n - k + 2, \dots, n + 1\}$ by using the general formula of w .

$$w_{k+1} = w_k p_{n-k+1} + \left(\prod_{i=n-k+2}^{n+1} p_i \right) [1 : p_{n-k+1} - 1].$$

■

7 Proof of Lemma 3.4

The lemma will be proven by using induction method. Let check the formula for $n = 2$

The set of co-prime numbers with the two primes 2 and 3 is defined as $V_{\text{mod}(2*3)} = \{1, 5\}$ then $\Delta V_{\text{mod}(2*3)} = \{0, 2, 4\}_{\text{mod}(2*3)}$.

From Theorem 3.1, we have that

$$V_{mod(2*3*5)} = (5 * V_{mod(2*3)} + 2 * 3[1 : 4])_{mod(2*3*5)} = \{1, 7, 11, 13, 17, 19, 23, 29\}$$

Therefore

$$U_{\{2*3*5\}} = \{1, 7, 11, 13, 17, 19, 23\} \Rightarrow (\Delta U_{\{2*3*5\}})_{mod(2*3*5)} = [0 : 2 : 6].$$

From lemma 3.2, the two important equations can be extracted

$$\begin{cases} V_{\prod_{i=1}^{n+1} p_i} = (p_{n+1} V_{\prod_{i=1}^n p_i} + \prod_{i=1}^n p_i [1 : p_{n+1} - 1])_{mod(\prod_{i=1}^{n+1} p_i)} \\ \text{and} \\ (p_{n+1} V_{\prod_{i=1}^n p_i})_{mod(\prod_{i=1}^n p_i)} = V_{\prod_{i=1}^n p_i}. \end{cases} \quad (10)$$

The set $U_{\prod_{i=1}^{n+1} p_i}$ is defined as an intersection of the set $V_{\prod_{i=1}^{n+1} p_i}$ and the interval $[0, 4 \prod_{i=1}^n p_i]$, i.e.,

$$U_{\prod_{i=1}^{n+1} p_i} = V_{\prod_{i=1}^{n+1} p_i} \cap \left[0 : 4 \prod_{i=1}^n p_i \right].$$

For all element i in the set $V_{\prod_{i=1}^n p_i}$, it exists unique element j , different from i , in $V_{\prod_{i=1}^n p_i}$ and an integer $k_0 \in \mathbb{N}$ such that

$$ip_{n+1} = j + k_0 \prod_{i=1}^n p_i,$$

which it leads to the following equation

$$p_{n+1} V_{\prod_{i=1}^n p_i} = \bigcup_{i=0}^{p_{n+1}-1} \Omega_i,$$

where $\Omega_i = \{y : i \prod_{i=1}^n p_i < y < (i+1) \prod_{i=1}^n p_i, \exists j \in V_{\prod_{i=1}^n p_i} \text{ where } jp_{n+1} = y\}$.
or just simply by

$$\Omega_i = p_{n+1} V_{\prod_{i=1}^n p_i} \cap [i \prod_{i=1}^n p_i, (i+1) \prod_{i=1}^n p_i].$$

Then the set $V_{\prod_{i=1}^{n+1} p_i}$ can be decomposed in terms of Ω_i as follows:

$$V_{\prod_{i=1}^{n+1} p_i} = \left(p_{n+1} V_{\prod_{i=1}^n p_i} + \prod_{i=1}^n p_i [1 : p_{n+1} - 1] \right)_{mod(\prod_{i=1}^{n+1} p_i)} \quad (11)$$

$$= \left(\bigcup_{i=0}^{p_{n+1}-1} \Omega_i + \prod_{i=1}^n p_i [1 : p_{n+1} - 1] \right)_{mod(\prod_{i=1}^{n+1} p_i)} \quad (12)$$

$$= \bigcup_{i=0}^{p_{n+1}-1} \left(i \left(\prod_{i=1}^n p_i \right) + \bigcup_{l=0, l \neq i}^{p_{n+1}-1} (\Omega_l)_{mod(\prod_{i=1}^n p_i)} \right)_{mod(\prod_{i=1}^{n+1} p_i)} \quad (13)$$

To make the notation easier to deal with, let define the following sets

$$W_i = \left(i \left(\prod_{j=1}^n p_j \right) + \bigcup_{l=0, l \neq i}^{p_{n+1}-1} (\Omega_l)_{\text{mod}(\prod_{j=1}^n p_j)} \right),$$

then

$$V_{\prod_{i=1}^{n+1} p_i} = \bigcup_{i=0}^{p_{n+1}-1} W_i.$$

From the properties of the co-primes that for all element x in $V_{\prod_{i=1}^n p_i}$ then the element $\prod_{i=1}^n p_i - x$ is also in $V_{\prod_{i=1}^n p_i}$, the below equation can be concluded

$$W_0 \cup (\Omega_0)_{\text{mod}(\prod_{i=1}^n p_i)} = V_{\prod_{i=1}^n p_i} \quad (14)$$

and

$$(\Omega_0)_{\text{mod}(\prod_{i=1}^n p_i)} = \left(\prod_{i=1}^n p_i - \Omega_{p_{n+1}-1} \right)_{\text{mod}(\prod_{i=1}^n p_i)}$$

In general we can write

$$\left(W_i \cup \left(W_{i+1} - \prod_{j=1}^n p_j \right) \right)_{\text{mod}(\prod_{j=1}^n p_j)} = V_{\prod_{j=1}^n p_j},$$

and for any two different integers i and j we can write

$$\left(W_i \cup \left(W_j - (j-i) \prod_{j=1}^n p_j \right) \right)_{\text{mod}(\prod_{j=1}^n p_j)} = V_{\prod_{j=1}^n p_j}.$$

Then we can write that

$$\Delta \left(V_{\prod_{i=1}^{n+1} p_i} \cap [0, 2 \prod_{i=1}^n p_i] \right) \supseteq (\Delta (V_{\prod_{i=1}^n p_i}))_{\text{mod}(\prod_{i=1}^n p_i)}.$$

In order to omit the $\text{mod}(\prod_{i=1}^n p_i)$ from our previous question, it is important to deal with the negative values in different ways.

For that, we need to prove that for all x and y are in $V_{\prod_{i=1}^n p_i}$, than $|x - y|$ and $-|y - x| + \prod_{i=1}^n p_i$ are both in $(\Delta U_{\prod_{i=1}^{n+1} p_i})$.

It leads from equation 14 that x and y belong to at least three sets from W_0, W_1, W_2 , and W_3 , i.e.,

$$\text{If } x \notin W_1 \Rightarrow x - \prod_{i=1}^n p_i \in W_0, \prod_{i=1}^n p_i - x \in W_1, x + \prod_{i=1}^n p_i \in W_2, \text{ and } x + 2 \prod_{i=1}^n p_i \in W_3$$

or

$$\text{If } y \notin W_2 \Rightarrow y - 2 \prod_{i=1}^n p_i \in W_0, x - \prod_{i=1}^n p_i \in W_1, \prod_{i=1}^n p_i - y \in W_2 \text{ and } x + \prod_{i=1}^n p_i \in W_3$$

In general for $j = \{i - 2, i - 1, i + 1, i + 2\}$ we have the following implication

$$\text{if } x + i \prod_{i=1}^n p_i \notin W_i \Rightarrow x + j \prod_{i=1}^n p_i \in W_j,$$

In order to cover all cases, it is enough to consider the set U as follows

$$U_{\prod_{i=1}^{n+1} p_i} = W_0 \cup W_1 \cup W_2 \cup W_3 \cup W_4$$

Now it is clear to observe that

$$\left(\Delta U_{\prod_{i=1}^{n+1} p_i} \right)_{\text{mod}(\prod_{i=1}^{n+1} p_i)} \supseteq \left(\Delta V_{\prod_{i=1}^n p_i} \right)_{\text{mod}(\prod_{i=1}^n p_i)} \quad (15)$$

$$\left(\Delta U_{\prod_{i=1}^{n+1} p_i} \right) \supseteq \left[0 : 2 : \prod_{i=1}^n p_i - 2 \right] \quad (16)$$

■

8 Proof of Lemma 3.5

Let start with a small examples to make all properties clear as it is indicated by follows

From Theorem 3.1, the co-prime sets can be calculated as following

$$V_{2*3} = \{1, 5\},$$

$$V_{2*3*5} = \{1, 7, 11, 13, 17, 19, 23, 29\},$$

$$V_{2*3*5*7} = \{1, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 59, 61, 67, \dots, 197, 199, 209\}.$$

By simple calculation we can find the following results

$$(\Delta V_{2*3*5})_{\text{mod}(2*3*5)} = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28\}.$$

$$(\Delta V_{2*3*5*7})_{\text{mod}(2*3*5*7)} = \{0, 2, 4, \dots, 206, 208\}.$$

$$\Delta U_{2*3*5*7}^1 = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28\}.$$

$$\Delta U_{2*3*5*7*11}^1 = \{0, 2, 4, \dots, 206, 208\}.$$

$$\Delta U_{2*3*5*7*11}^2 = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28\}.$$

$$\Delta U_{2*3*5*7*11*13}^3 = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28\}.$$

$$\Delta U_{2*3*5*7*11*13*17*19*23}^5 = \{0, 2, 4, \dots, 206, 208\}.$$

To make this result general, we will proceed to prove the first part of this lemma by using the Theorem 3.1, for which it gives that for all $n > 2$:

$$V_{\prod_{i=1}^{n+1} p_i} = \left(p_{n+1} V_{\prod_{i=1}^n p_i} + \left(\prod_{i=1}^{n+1} p_i \right) [1 : p_{n+1} - 1] \right)_{\text{mod}(\prod_{i=1}^{n+1} p_i)}.$$

In order to track the evolution of the co-prime sets, we will define

$$\Psi_i = V_{\prod_{i=1}^n p_i} \cap \left[i \frac{\prod_{i=1}^n p_i}{p_{n+1}} : (i+1) \frac{\prod_{i=1}^n p_i}{p_{n+1}} \right],$$

then we can write

$$V_{\prod_{i=1}^{n+1} p_i} = \left(p_{n+1} \left(\bigcup_{i=0}^{p_{n+1}-1} \Psi_i \right) + \left(\prod_{i=1}^{n+1} p_i \right) [1 : p_{n+1} - 1] \right)_{\text{mod}(\prod_{i=1}^{n+1} p_i)} \quad (17)$$

Let define for instant the set

$$U_{\prod_{i=1}^{n+1} p_i}^1 = V_{\prod_{i=1}^{n+1} p_i} \cap [0 : \prod_{i=1}^n p_i]$$

and we will explain later why we need to enlarge the set U^1 by double.

We can find out that $\left(\Delta U_{\prod_{i=1}^{n+1} p_i}^1 \right)_{\text{mod}(\prod_{i=1}^n p_i)} = \left(\Delta V_{\prod_{i=1}^n p_i} \right)_{\text{mod}(\prod_{i=1}^n p_i)}$ because of the following properties

- The set $U_{\prod_{i=1}^{n+1} p_i}^1$ contains all elements inside $V_{\prod_{i=1}^n p_i}$ except multiples of p_{n+1} then $U_{\prod_{i=1}^{n+1} p_i}^1 \subseteq V_{\prod_{i=1}^{n+1} p_i}$, and the missing numbers are only multiples of p_{n+1} represented by the set $p_{n+1} \Psi_0$.
- If x is multiple of p_{n+1} then $(\prod_{i=1}^n p_i) - x$ is not a multiple of p_{n+1} , so we can find out that if the value x is not in $U_{\prod_{i=1}^{n+1} p_i}^1$ and it in $V_{\prod_{i=1}^n p_i}$ then

$$\left(\prod_{i=1}^n p_i \right) - x \in U_{\prod_{i=1}^{n+1} p_i}^1.$$

This result comes from the impossibility to have both x and $(\prod_{i=1}^n p_i) - x$ as multiple of p_{n+1} which it leads to a contradiction

$$\frac{(\prod_{i=1}^n p_i)}{p_{n+1}} \in \mathbb{Z}.$$

- From equation 17, we can conclude that for all $x \in V_{\prod_{i=1}^{n-1} p_i}$, it exists a unique integer $l < p_n$ such that

$$(x)_{\text{mod}(\prod_{i=1}^{n-1} p_i)} \notin \left(V_{\prod_{i=1}^n p_i} \cap \left[l \prod_{i=1}^{n-1} p_i, (l+1) \prod_{i=1}^{n-1} p_i \right] \right)_{\text{mod}(\prod_{i=1}^{n-1} p_i)}.$$

This result can be found out from the cardinality of the sets

$$\text{Card}(V_{\prod_{i=1}^{n-1} p_i}) = \text{Card}(V_{\prod_{i=1}^{n-2} p_i})(p_{n-1} - 1) = \prod_{i=2}^n (p_i - 1),$$

or from the theorem 3.1 and Lemma 3.2, i.e.,

$$\left\{ x + l \prod_{i=1}^{n-1} p_i : l = 0, 1, \dots, p_n - 1 \right\}$$

has at most one element which it is a multiple of p_n .

By using the above properties, we can prove that for all x and y inside the set $V_{\prod_{i=1}^n p_i}$ then we can prove easily that $(x-y)_{\text{mod}(\prod_{i=1}^n p_i)}$ and $(y-x)_{\text{mod}(\prod_{i=1}^n p_i)}$ are both inside $\left(\Delta U_{\prod_{i=1}^{n+1} p_i}^1 \right)_{\text{mod}(\prod_{i=1}^n p_i)}$. To do that it is enough to consider only the cases where x or y are multiple of p_{n+1} , i. e. belong to $\Psi_0 p_{n+1}$. All cases are checked as it is indicated below

Case 1 If $x \notin U_{\prod_{i=1}^{n+1} p_i}^1$, $y \in U_{\prod_{i=1}^{n+1} p_i}^1$, and $\prod_{i=1}^n p_i - y \in U_{\prod_{i=1}^{n+1} p_i}^1$ then $\prod_{i=1}^n p_i - x \in U_{\prod_{i=1}^{n+1} p_i}^1$ so we have

$$\begin{aligned} \left(\left(\prod_{i=1}^n p_i - x \right) - \left(\prod_{i=1}^n p_i - y \right) \right)_{\text{mod}(\prod_{i=1}^n p_i)} &= (y - x)_{\text{mod}(\prod_{i=1}^n p_i)} \\ \left(\left(\prod_{i=1}^n p_i - y \right) - \left(\prod_{i=1}^n p_i - x \right) \right)_{\text{mod}(\prod_{i=1}^n p_i)} &= (x - y)_{\text{mod}(\prod_{i=1}^n p_i)}. \end{aligned}$$

Case 2 If $x \notin U_{\prod_{i=1}^{n+1} p_i}^1$, $y \in U_{\prod_{i=1}^{n+1} p_i}^1$, and $\prod_{i=1}^n p_i - y \notin U_{\prod_{i=1}^{n+1} p_i}^1$ then from decomposition of $V_{\prod_{i=1}^n p_i}$ in function of $V_{\prod_{i=1}^{n-1} p_i}$ so it exist an integer $l < p_n$ such that $x + l \prod_{i=1}^{n-1} p_i$ and $y + l \prod_{i=1}^{n-1} p_i$, in modulo $\prod_{i=1}^n p_i$, are inside $U_{\prod_{i=1}^{n+1} p_i}^1$ then

$$\left(\left(l \prod_{i=1}^{n-1} p_i + y \right) - \left(l \prod_{i=1}^{n-1} p_i + x \right) \right)_{\text{mod}(\prod_{i=1}^n p_i)} = (y - x)_{\text{mod}(\prod_{i=1}^n p_i)}$$

$$\left(\left(l \prod_{i=1}^{n-1} p_i + x \right) - \left(l \prod_{i=1}^{n-1} p_i + y \right) \right)_{\text{mod}(\prod_{i=1}^n p_i)} = (x - y)_{\text{mod}(\prod_{i=1}^n p_i)}.$$

This result can be justified by the fact that it not possible to find two integers less than p_n , l_1 and l_2 , such that

$$\left(l_1 \prod_{i=1}^{n-1} p_i + x \right)_{\text{mod}(p_j)} = \left(l_2 \prod_{i=1}^{n-1} p_i + x \right)_{\text{mod}(p_j)} = 0,$$

where j equals to n or $n + 1$.

Case 3 If $x \notin U_{\prod_{i=1}^{n+1} p_i}^1$ and $y \notin U_{\prod_{i=1}^{n+1} p_i}^1$ then $\prod_{i=1}^n p_i - x \in U_{\prod_{i=1}^{n+1} p_i}^1$ and $\prod_{i=1}^n p_i - y \in U_{\prod_{i=1}^{n+1} p_i}^1$ so again

$$\begin{aligned} \left(\left(\prod_{i=1}^n p_i - x \right) - \left(\prod_{i=1}^n p_i - y \right) \right)_{\text{mod}(\prod_{i=1}^n p_i)} &= (y - x)_{\text{mod}(\prod_{i=1}^n p_i)} \\ \left(\left(\prod_{i=1}^n p_i - y \right) - \left(\prod_{i=1}^n p_i - x \right) \right)_{\text{mod}(\prod_{i=1}^n p_i)} &= (x - y)_{\text{mod}(\prod_{i=1}^n p_i)}. \end{aligned}$$

After what it said above, we can conclude that

$$\begin{aligned} \left(\Delta U_{\prod_{i=1}^{n+1} p_i}^1 \right)_{\text{mod}(\prod_{i=1}^n p_i)} &= \left(\Delta V_{\prod_{i=1}^n p_i} \right)_{\text{mod}(\prod_{i=1}^n p_i)} \\ &= [0 : 2 : \prod_{i=1}^n p_i - 2]. \end{aligned}$$

By the same way we can find also that for all $j < p_{n+1}$

$$\left(\Delta U_{\prod_{i=1}^{n+1} p_i}^{1,j} \right)_{\text{mod}(\prod_{i=1}^n p_i)} = \left(\Delta V_{\prod_{i=1}^n p_i} \right)_{\text{mod}(\prod_{i=1}^n p_i)},$$

where $U_{\prod_{i=1}^{n+1} p_i}^{1,j} = V_{\prod_{i=1}^{n+1} p_i} \cap [j \prod_{i=1}^n p_i : (j+1) \prod_{i=1}^n p_i]$.

By using the same approach, the first part of our lemma can be derived when $x \in V_{\prod_{i=1}^n p_i}$ and $y \in l \prod_{i=1}^n p_i + V_{\prod_{i=1}^n p_i}$, where l is any integer number less than p_{n+1}

$$\left(\Delta V_{\prod_{i=1}^{n+1} p_i} \right)_{\text{mod}(\prod_{i=1}^{n+1} p_i)} = \left(\Delta U_{\prod_{i=1}^{n+1} p_i}^1 \right)_{\text{mod}(\prod_{i=1}^n p_i)} + \left(\prod_{i=1}^n p_i \right) [0 : 1 : p_{n+1} - 1].$$

We suggest to prove the formula for $k = 2$ in order to make the generalization easier. Let's start by highlighting some extremely important properties, which they are derived from the symmetry of the set $V_{\prod_{i=1}^{n-1} p_i}$, i.e.,

$$\forall x \in V_{\prod_{i=1}^{n-1} p_i} \Rightarrow \prod_{i=1}^{n-1} p_i - x \in V_{\prod_{i=1}^{n-1} p_i}$$

and from the recurrence equation

$$V_{\prod_{i=1}^n p_i} = p_n V_{\prod_{i=1}^{n-1} p_i} + \left(\prod_{i=1}^{n-1} p_i \right) [1 : p_n - 1].$$

These properties link between elements of $V_{\prod_{i=1}^{n-1} p_i}$ and $U_{\prod_{i=1}^{n+1} p_i}^2$ as follows
For all $x \in V_{\prod_{i=1}^{n-1} p_i}$, it exists an integer set L such that for all $l \in L$ we have

$$\left(l \left(\prod_{i=1}^{n-2} p_i \right) + x_{\text{mod}(\prod_{i=1}^{n-2} p_i)} \right)_{\text{mod}(\prod_{i=1}^{n-1} p_i)} \in U_{\prod_{i=1}^{n+1} p_i}^2,$$

where $\text{Card}(L \cap [0 : 1 : p_{n-1} - 1]) \geq p_{n-1} - 2$.

This statement comes from the fact that, for all integer $i \in \{0, 1, 2\}$, it is not possible to find more than one integer from the set

$$\Upsilon_n^2 = \left\{ l \left(\prod_{i=1}^{n-2} p_i \right) + x : l < p_{n-1} \right\},$$

which are multiple of p_{n-1+i} . i.e.,

$$\text{card} \left(\Upsilon_n^2 \cup \{I \in \mathbb{N} : I_{\text{mod}(p_{n-1+i})} = 0\} \right) \leq 1. \quad (18)$$

Therefore, by the pigeonhole principle we can conclude the following

$$\forall (x, y) \in \left(V_{\prod_{i=1}^{n-1} p_i} \right)^2 \Rightarrow \exists l \in \mathbb{Z} : \left\{ x + l \prod_{i=1}^{n-2} p_i, y + l \prod_{i=1}^{n-2} p_i \right\}_{\text{mod}(\prod_{i=1}^{n-1} p_i)} \subseteq U_{\prod_{i=1}^{n+1} p_i}^2,$$

which implies that

$$\begin{aligned} \left(\Delta U_{\prod_{i=1}^{n+1} p_i}^2 \right)_{\text{mod}(\prod_{i=1}^{n-1} p_i)} &= \left(\Delta V_{\prod_{i=1}^{n-1} p_i} \right)_{\text{mod}(\prod_{i=1}^{n-1} p_i)} \\ &= \left(\Delta U_{\prod_{i=1}^{n+1} p_i}^{2,j} \right)_{\text{mod}(\prod_{i=1}^{n-1} p_i)} \\ &= [0 : 2 : \prod_{i=1}^{n-1} p_i - 2] \end{aligned}$$

and also for all $j \in \{0, 1, \dots, p_n p_{n_1} - 1\}$

$$\left(\Delta U_{\prod_{i=1}^{n+1} p_i}^2 \right)_{\text{mod}(\prod_{i=1}^{n-1} p_i)} = \left(\Delta U_{\prod_{i=1}^{n+1} p_i}^{2,j} \right)_{\text{mod}(\prod_{i=1}^{n-1} p_i)}.$$

Then we can write

$$\begin{aligned} \left(\Delta V_{\prod_{i=1}^{n+1} p_i} \right)_{\text{mod}(\prod_{i=1}^{n+1} p_i)} &= \left(\Delta U_{\prod_{i=1}^{n+1} p_i}^2 \right)_{\text{mod}(\prod_{i=1}^{n+1} p_i)} + \left(\prod_{i=1}^{n-1} p_i \right) [0 : 1 : p_n - 1] \\ &+ \left(\prod_{i=1}^n p_i \right) [0 : 1 : p_{n+1} - 1]. \end{aligned}$$

By the same way we can generalize our above result to conclude that

$$\begin{aligned} \left(\Delta U_{\prod_{i=1}^{n-k+1} p_i}^{k+1} \right)_{\text{mod}(\prod_{i=1}^{n-k} p_i)} &= \left(\Delta V_{\prod_{i=1}^{n-k} p_i} \right)_{\text{mod}(\prod_{i=1}^{n-k} p_i)} \\ &= \left(\Delta U_{\prod_{i=1}^{n-k+1} p_i}^{k+1, j} \right)_{\text{mod}(\prod_{i=1}^{n-k} p_i)} \\ &= [0 : 2 : \prod_{i=1}^{n-k} p_i - 2], \end{aligned}$$

where the value of k should verify the following condition

$$k + 1 < \frac{p_{n-k}}{2}. \quad (19)$$

This condition comes from the facts that

- For all $j \in \{0, 1, 2, \dots, k, k+1\}$ and for all $x \in \prod_{i=1}^{n-k} p_i$, we have the following fact

$$\text{Card} \left(\Upsilon_n^{k+1} \cap \{J \in \mathbb{N} : J_{\text{mod}(p_{n-k+j})} = 0\} \right) \leq 1,$$

where $x_0 = x_{\text{mod}(\prod_{i=1}^{n-k-1} p_i)}$ and $\Upsilon_n^{k+1} = \left\{ l \left(\prod_{i=1}^{n-k-1} p_i \right) + x_0 : l < p_{n-k} \right\}$

- For all $x \in V_{\prod_{i=1}^{n-k} p_i}$, it exists a set of integers, L , such that for all $l \in L$ we have

$$\left(l \left(\prod_{i=1}^{n-k-1} p_i \right) + x_0 \right)_{\text{mod}(\prod_{i=1}^{n-k} p_i)} \in U_{\prod_{i=1}^{n+1} p_i}^{k+1},$$

where $\text{Card}(L) \cap [0 : 1 : p_{n-k} - 1] \geq p_{n-k} - k - 1$.

- The Pigeonhole Principle to conclude these facts if $k + 1 < \frac{p_{n-k}}{2}$.

We would like to investigate if we can push the condition 19 further, i.e., can we generalize our result for all $k < k_0$, for where $\prod_{i=1}^{n-k_0} p_i < p_{n+1}^2$ and $\prod_{i=1}^{n-k_0} p_i > p_{n+1}$ in order to ensure that set is not empty and contains only primes?

Our target is to push the condition 19 more further, i.e., $k_0 > \frac{p_{n-k}}{2}$, so we will prove that for all $k + m < k_0$ and for all $(x, y) \in \left(V_{\prod_{i=1}^{n-k} p_i}\right)^2$ then it exists $l \in \mathbb{Z}$ such that

$$\left\{ x + l \prod_{i=1}^{n-k-m} p_i, y + l \prod_{i=1}^{n-k-m} p_i \right\}_{\text{mod}(\prod_{i=1}^{n-k} p_i)} \subseteq \left(U_{\prod_{i=1}^{n+1} p_i}^{k+1} \right)^2 \quad (20)$$

In order to prove the previous equation some definitions and statement will be introduced to facilitate the explanation, then for all $(x, y) \in \left(V_{\prod_{i=1}^{n-k} p_i}\right)^2$ we define the following items

- let $x_0 = x_{\text{mod}(\prod_{i=1}^{n-k-m} p_i)}$ and $y_0 = y_{\text{mod}(\prod_{i=1}^{n-k-m} p_i)}$
- let $V_{\prod_{i=1}^{n-k} p_i} = \left(V_{\prod_{i=1}^{n-k-m} p_i} + \prod_{i=1}^{n-k-m} p_i [0 : 1 : \prod_{i=n-k-m+1}^{n-k} p_i] \right) / M_{\prod_{i=n-k-m+1}^{n+1} p_i}$, where $M_{\prod_{i=n-k-m+1}^{n+1} p_i}$ is a set of elements that are multiples of $p_{n-k-m+1}$ or $p_{n-k-m+2}$ or...or p_{n+1}
- let define the vector $H_x = (x_0, x_0 + \prod_{i=1}^{n-k-m} p_i, \dots, x_0 + l_x \prod_{i=1}^{n-k-m} p_i)$, where $l_x = \prod_{i=n-k-m+1}^{n-k} p_i - 1$.
- let define the vector $H_y = (y_0, y_0 + \prod_{i=1}^{n-k-m} p_i, \dots, y_0 + l_y \prod_{i=1}^{n-k-m} p_i)$, where $l_y = \prod_{i=n-k-m+1}^{n-k} p_i - 1$.
- For $j \in \{1, 2, \dots, k+m\}$ and for $l \in \mathbb{N}$, if $\left(x_0 + l \prod_{i=1}^{n-k-m} p_i \right)_{\text{mod}(p_{n+1-j})} = 0$ then

$$\left(x_0 + (l \pm p_{n+1-j}) \prod_{i=1}^{n-k-m} p_i \right)_{\text{mod}(p_{n+1-j})} = 0.$$

From the equation 18 and from the pigeonhole principle we can make ensure about the existence of $l \in \mathbb{Z} : x_0 + l \prod_{i=1}^{n-k-m} p_i \in H_x$, and $y_0 + l \prod_{i=1}^{n-k-m} p_i \in H_y$, e.i., the existence of $l' \in \mathbb{Z}$ such that $(x + l' \prod_{i=1}^{n-k-m} p_i, y + l' \prod_{i=1}^{n-k-m} p_i) \in U_{\prod_{i=1}^{n+1} p_i}^{k+1}$ by choosing the right integers m and k such that

$$\text{Card} \{ l \in H_x : \forall i \in [n-k-m+1 : 1 : n+1], \gcd(l, p_i) = 1 \} > \frac{\prod_{i=n-k-m+1}^{n-k} p_i}{2}.$$

By using Chinese remainder theorem, the density of co-primes, Lemma 3.6, and $p_{n-k} \sim (n-k) \ln(n-k)$ to show that for $n-k$ big enough and for m equals to two we have the following steps

Step 1 if $\left(x_0 + l_j \prod_{i=1}^{n-k-2} p_i \right)_{\text{mod}(p_{n+1-j})} = 0$ then for $i \in \{0, 1, 2, \dots, p_{n+1-j}\}$

$$\left(x_0 + (l_j + i) \prod_{i=1}^{n-k-2} p_i \right)_{\text{mod}(p_{n+1-j})} \neq 0$$

and

$$\left(x_0 + (l_j + p_{n+1-j}) \prod_{i=1}^{n-k-2} p_i \right)_{\text{mod}(p_{n+1-j})} = 0.$$

Step 2 The existence of an integer number, Γ , such that

$$\begin{aligned} (\Gamma)_{\text{mod}(p_{n+1})} &= p_{n+1} - (l_{n+1})_{\text{mod}(p_{n+1})} \\ (\Gamma)_{\text{mod}(p_n)} &= p_n - (l_n)_{\text{mod}(p_n)} \\ (\Gamma)_{\text{mod}(p_{n-1})} &= p_{n-1} - (l_{n-1})_{\text{mod}(p_{n-1})} \\ &\vdots \\ (\Gamma)_{\text{mod}(p_{n-k-1})} &= p_{n-k-1} - (l_{n-k-1})_{\text{mod}(p_{n-k-1})} \end{aligned}$$

is assured by the Chinese remainder Theorem.

Step 3 By consequence, for any positive integer u we have the following

$$\text{Card}(l \in H'_x) \sim \text{Card} \left(\Gamma_u \leq j \leq \Gamma_u + \prod_{i=n-k-1}^{n-k} p_i \mid \forall i \in \{n-k-1, \dots, n+1\} \text{ gcd}(j, p_i) = 1 \right),$$

where $H'_x = \{l \in H_x \mid \forall i \in [n-k-1 : 1 : n+1] : \text{gcd}(l, p_i) = 1\}$ and $\Gamma_u = \Gamma + u \prod_{i=n-k-1}^{n+1} p_i$.

Step 4 If $Q = \{p_i : n-k-1 \leq i \leq n+1\}$, then by using Lemma 3.6 or the appendix we can write the following

$$\begin{aligned} \text{Card}\{l \in H'_x\} &= \Psi(\Gamma_u + p_{n-k-1}p_{n-k}, p_{n-k-2}, Q) - \Psi(\Gamma_u + p_{n-k-2}, p_{n-k-2}, Q) \\ &= \Psi(p_{n-k-1}p_{n-k}, p_{n-k-2}, Q) - p_{n-k-2} \\ &\sim (p_{n-k-1}p_{n-k} - p_{n-k-2}) \left(\frac{\ln(n-k-2)}{\ln(n-k-1)(n-k)} \right) \\ &\sim \ln(n-k-2) \frac{p_{n-k-1}p_{n-k}}{\ln((n-k-1)(n-k))} \\ &\sim \frac{p_{n-k-1}p_{n-k}}{2} \end{aligned}$$

Therefore, it concludes for all $k \geq k_0$, where k_0 is smallest value that verify $\prod_{i=1}^{n-k-2} p_i > p_{n+2}$, that

$$\left(\Delta V_{\prod_{i=1}^{n+1} p_i} \right)_{\text{mod}(\prod_{i=1}^{n+1} p_i)} = \left(\Delta V_{\prod_{i=1}^{n+1-k} p_i} \right)_{\text{mod}(\prod_{i=1}^n p_i)} + \sum_{j=0}^{k-1} \left(\prod_{i=1}^{n-j} p_i \right) [0 : 1 : p_{n+1-j}-1] \quad (21)$$

and

$$\left(\Delta V_{\prod_{i=1}^{n+1} p_i}\right)_{\text{mod}(\prod_{i=1}^{n+1} p_i)} = \left(\Delta U_{\prod_{i=1}^{n+1} p_i}^k\right)_{\text{mod}(\prod_{i=1}^{n+1-k} p_i)} + \sum_{j=0}^{k-1} \left(\prod_{i=1}^{n-j} p_i\right) [0 : 1 : p_{n+1-j} - 1]. \quad (22)$$

From Lemma 3.3 we can write

$$\begin{aligned} \left(\Delta U_{\prod_{i=1}^{n+1} p_i}^k\right)_{\text{mod}(\prod_{i=1}^{n+1} p_i)} &= \left(\Delta U_{\prod_{i=1}^{n+1} p_i}^{k,j}\right)_{\text{mod}(\prod_{i=1}^{n+1} p_i)} \\ &= \left(\Delta V_{\prod_{i=1}^{n+1-k} p_i}\right)_{\text{mod}(\prod_{i=1}^{n+1-k} p_i)} \\ &= [0 : 2 : \left(\prod_{i=1}^{n+1-k} p_i\right) - 2]. \end{aligned}$$

In order to omit the modulo from the previous equation, it will be enough to enlarge the set U by a double. The calculation in modulo $\prod_{i=1}^n p_i$ will add $\prod_{i=1}^n p_i$ to the negative value, this idea will be used to prove the formula for the case $k = 1$

$$\left(\Delta U_{\prod_{i=1}^{n+1} p_i}^1\right) = \left(\Delta V_{\prod_{i=1}^{n+1} p_i}\right)_{\text{mod}(\prod_{i=1}^n p_i)},$$

We have the following facts:

- $V_{\prod_{i=1}^{n+1} p_i} \cap [0 : \prod_{i=1}^n p_i] = \bigcup_{j=1}^{p_{n+1}-1} \Psi_j$.
- $V_{\prod_{i=1}^{n+1} p_i} \cap [\prod_{i=1}^n p_i : 2 \prod_{i=1}^n p_i] = (\Psi_0 + \prod_{i=1}^n p_i) \cup \left(\bigcup_{j=2}^{p_{n+1}-1} (\Psi_j + \prod_{i=1}^n p_i)\right)$.
- Ψ_0 is set of integers which are multiples of p_{n+1} and belong to $V_{\prod_{i=1}^n p_i}$.
- In general Ψ_j are sets of entegers which are multiples of p_{n+1} and belong to $V_{\prod_{i=1}^n p_i} + j \prod_{i=1}^n p_i$, for $j = 0, 1, \dots, p_{n+1} - 1$.
- If $x \in \Psi_0$ which means that $x_{\text{mod}(p_{n+1})} = 0$ then $x + \prod_{i=1}^n p_i$ and $2 \prod_{i=1}^n p_i - x$ both belong to $V_{\prod_{i=1}^{n+1} p_i} \cap [\prod_{i=1}^n p_i : 2 \prod_{i=1}^n p_i]$.
- If $x \in \Psi_1$ which means that $(x + \prod_{i=1}^n p_i)_{\text{mod}(p_{n+1})} = 0$ then x and $\prod_{i=1}^n p_i - x$ both belong to $V_{\prod_{i=1}^{n+1} p_i} \cap [0 : \prod_{i=1}^n p_i]$.

The question is how to make sure that for all x and y inside $\bigcup_{j=1}^{p_{n+1}-1} \Psi_j$ such that $x - y < 0$ then $x + \prod_{i=1}^n p_i$ or $y - \prod_{i=1}^n p_i$ belong to $V_{\prod_{i=1}^{n+1} p_i} \cap [0 : 2 \prod_{i=1}^n p_i]$, i.e., $x - y + \prod_{i=1}^n p_i \in \Delta U_{\prod_{i=1}^{n+1} p_i}^1$.

To answer this question, we have to check the following cases

Case 1 If x and y belong to $\bigcup_{j=2}^{p_{n+1}-1} \Psi_j$ then $x + \prod_{i=1}^n p_i$, $y + \prod_{i=1}^n p_i$ belong to $V_{\prod_{i=1}^{n+1} p_i} \cap [0 : \prod_{i=1}^n p_i]$. So $x - y + \prod_{i=1}^n p_i \in \Delta U_{\prod_{i=1}^{n+1} p_i}^1$.

Case 2 If x and y belong to Ψ_0 then $\prod_{i=1}^n p_i - x$ and $\prod_{i=1}^n p_i - y$ belong to $\bigcup_{j=1}^{p_{n+1}-1} \Psi_j$ and also $x + \prod_{i=1}^n p_i$, $y + \prod_{i=1}^n p_i$, $2 \prod_{i=1}^n p_i - x$, and $2 \prod_{i=1}^n p_i - y$ belong to $V_{\prod_{i=1}^{n+1} p_i} \cap [\prod_{i=1}^n p_i : 2 \prod_{i=1}^n p_i]$. So $x - y + \prod_{i=1}^n p_i \in \Delta U_{\prod_{i=1}^{n+1} p_i}^1$.

Case 3 If x and y belong to Ψ_1 then x , y , $\prod_{i=1}^n p_i - x$, and $\prod_{i=1}^n p_i - y$ belong to $\bigcup_{j=1}^{p_{n+1}-1} \Psi_j$ and also $2 \prod_{i=1}^n p_i - x$, and $2 \prod_{i=1}^n p_i - y$ belong to $V_{\prod_{i=1}^{n+1} p_i} \cap [\prod_{i=1}^n p_i : 2 \prod_{i=1}^n p_i]$. So $x - y + \prod_{i=1}^n p_i \in \Delta U_{\prod_{i=1}^{n+1} p_i}^1$.

Case 4 If $x \in \Psi_1$ and $y \in \Psi_0$ then x , $x - \prod_{i=1}^n p_i$, and $\prod_{i=1}^n p_i - y$ belong to $\bigcup_{j=1}^{p_{n+1}-1} \Psi_j$ and also $2 \prod_{i=1}^n p_i - x$ and $y + \prod_{i=1}^n p_i$ belong to $V_{\prod_{i=1}^{n+1} p_i} \cap [\prod_{i=1}^n p_i : 2 \prod_{i=1}^n p_i]$. So $x - y + \prod_{i=1}^n p_i \in \Delta U_{\prod_{i=1}^{n+1} p_i}^1$.

Case 5 Other cases are trivial to be checked.

For the other cases of k can be derived by the same approach as we did to prove the equation 20, for $m = 2$, to prove that

$\forall x \in V_{\prod_{i=1}^{n-k} p_i}$ and $\forall y \in \prod_{i=1}^{n-k} p_i + V_{\prod_{i=1}^{n-k} p_i}$ then it exists $l \in \mathbb{Z}$ such that $(x + l \prod_{i=1}^{n-k-m} p_i) \in U_{\prod_{i=1}^{n+1} p_i}^{k+1}$ and $(y + l \prod_{i=1}^{n-k-m} p_i) \in U_{\prod_{i=1}^{n+1} p_i}^{k+1,1}$.

■

9 Proof of Lemma 3.6

Let $\pi(x, n)$ be the co-prime-counting function that gives the number of co-primes with $p_i, i > n$, and are less or equal to x and N be the rank of biggest prime less than the value x , we can observe easily that

$$\begin{aligned} \pi(x, 1) &= \pi(x) \\ \pi(x, N) &= x \end{aligned}$$

Number of co-primes with p_N and less than x is calculated by subtracting all multiples of p_N from x integers,

$$\pi(x, N-1) = x - \left\lfloor \frac{x}{p_N} \right\rfloor,$$

by the same way we can find number of co-primes with p_N and p_{N-1} can be calculated as

$$\pi(x, N-2) = x - \left\lfloor \frac{x}{p_N} \right\rfloor - \left\lfloor \frac{x}{p_{N-1}} \right\rfloor + \left\lfloor \frac{x}{p_N p_{N-1}} \right\rfloor,$$

where we simply this formula as

$$\pi(x, N-2) \sim x \left(1 - \frac{1}{p_N}\right) \left(1 - \frac{1}{p_{N-1}}\right).$$

By iteration, we can find $\pi(x, n)$ as follows

$$\pi(x, n) = x - \sum_{j=1}^N (-1)^j \left(\sum_{n+1 \leq i_1 < i_2 < \dots < i_j \leq N} \left\lfloor \frac{x}{\prod_{l=1}^j p_{i_l}} \right\rfloor \right)$$

We can generate it to

$$\Psi(x, y, Q) = x - \sum_{j=1}^{N_Q} (-1)^j \left(\sum_{1 \leq i_1 < i_2 < \dots < i_j \leq N_Q} \left\lfloor \frac{x}{\prod_{l=1}^j q_{i_l}} \right\rfloor \right), \quad (23)$$

where q_i are primes inside the set Q and $N_Q = \text{Card}(Q)$.

9.1 Proof of the first part of Lemma 3.6

The first part of Lemma 3.6 can be conducted by the fact that for all positive integer i and for all prime, $p \in Q$, we have

$$(y + i)_{\text{mod}(p)} = (y + kP_Q + i)_{\text{mod}(p)},$$

then

$$\Psi(x, y, Q) = \text{Card} \{i \in (y + kP_Q, x + kP_Q] \mid \gcd(i, P_Q) = 1\}.$$

9.2 Proof of the second part of Lemma 3.6

The second part of Lemma 3.6 can be proved by using the the equation 23 and the fact that for all integer x

$$\left\lfloor \frac{x + kP_Q}{\prod_{l=1}^j q_{i_l}} \right\rfloor = \left\lfloor \frac{x}{\prod_{l=1}^j q_{i_l}} \right\rfloor + \frac{kP_Q}{\prod_{l=1}^j q_{i_l}}$$

as follows

$$\begin{aligned} \Psi(x + kP_Q, y, Q) &= x + kP_Q - \sum_{j=1}^{N_Q} (-1)^j \left(\sum_{1 \leq i_1 < i_2 < \dots < i_j \leq N_Q} \left\lfloor \frac{x + kP_Q}{\prod_{l=1}^j q_{i_l}} \right\rfloor \right) \\ &= x + kP_Q - \sum_{j=1}^{N_Q} (-1)^j \left(\sum_{1 \leq i_1 < i_2 < \dots < i_j \leq N_Q} \left\lfloor \frac{x}{\prod_{l=1}^j q_{i_l}} \right\rfloor + \frac{kP_Q}{\prod_{l=1}^j q_{i_l}} \right) \end{aligned}$$

and

$$\begin{aligned}
\Psi(y + kP_Q, y, Q) &= y + kP_Q - \sum_{j=1}^{N_Q} (-1)^j \left(\sum_{1 \leq i_1 < i_2 < \dots < i_j \leq N_Q} \left\lfloor \frac{y + kP_Q}{\prod_{l=1}^j q_{i_l}} \right\rfloor \right) \\
&= y + kP_Q - \sum_{j=1}^{N_Q} (-1)^j \left(\sum_{1 \leq i_1 < i_2 < \dots < i_j \leq N_Q} \left\lfloor \frac{y}{\prod_{l=1}^j q_{i_l}} \right\rfloor + \frac{kP_Q}{\prod_{l=1}^j q_{i_l}} \right).
\end{aligned}$$

By Subtracting the last two equations we can find

$$\begin{aligned}
\Psi(x + kP_Q, y, Q) - \Psi(y + kP_Q, y, Q) &= x - \sum_{j=1}^{N_Q} (-1)^j \left(\sum_{1 \leq i_1 < i_2 < \dots < i_j \leq N_Q} \left\lfloor \frac{x}{\prod_{l=1}^j q_{i_l}} \right\rfloor \right) - y \\
&= \Psi(x, y, Q) - y,
\end{aligned}$$

where $\sum_{j=1}^{N_Q} (-1)^j \left(\sum_{1 \leq i_1 < i_2 < \dots < i_j \leq N_Q} \left\lfloor \frac{y}{\prod_{l=1}^j q_{i_l}} \right\rfloor \right) = 0$ since $y < \min(Q)$.

We can find also that if $x < P_Q$ and $\gcd(x, P_Q) = 1$ then

$$\Psi(x, y, Q) + \Psi(P_Q - x, y, Q) = \Psi(P_Q, y, Q) + 1 = P_Q \prod_{p_i \in Q} \left(1 - \frac{1}{p_i} \right).$$

Therefore, by using same the equation 23 we can write the following equations

$$\begin{aligned}
\Psi(P_Q - x, y, Q) + \Psi(y, y, Q) &= P_Q - \sum_{j=1}^{N_Q} (-1)^j \left(\sum_{1 \leq i_1 < i_2 < \dots < i_j \leq N_Q} \left\lfloor \frac{P_Q - x}{\prod_{l=1}^j q_{i_l}} + \frac{x}{\prod_{l=1}^j q_{i_l}} \right\rfloor \right) \\
&= - \sum_{j=1}^{N_Q} (-1)^j \left(\sum_{1 \leq i_1 < i_2 < \dots < i_j \leq N_Q} - \left\lfloor \frac{x}{\prod_{l=1}^j q_{i_l}} \right\rfloor + \left\lfloor \frac{x}{\prod_{l=1}^j q_{i_l}} \right\rfloor \right) \\
&\quad + P_Q - \sum_{j=1}^{N_Q} (-1)^j \left(\sum_{1 \leq i_1 < i_2 < \dots < i_j \leq N_Q} \frac{P_Q}{\prod_{l=1}^j q_{i_l}} \right) \\
&= P_Q - \sum_{j=1}^{N_Q} (-1)^j \left(\sum_{1 \leq i_1 < i_2 < \dots < i_j \leq N_Q} \frac{P_Q}{\prod_{l=1}^j q_{i_l}} \right) + 1 \\
&= P_Q \prod_{p_i \in Q} \left(1 - \frac{1}{p_i} \right) + 1
\end{aligned}$$

9.3 Proof of the third part of Lemma 3.6

The third part of Lemma 3.6 will be proved by improving Theorem 1 and the proposition 3 in [10] and [11], where it stated that: There is some δ , $0 \leq \delta < 1$, and some $A > 0$ such that

$$\sum_{\substack{p \leq x \\ p \in Q}} \ln(p) = \delta x + O(x \ln^{-A}(x)),$$

then

$$\Psi(x, y, Q) = \frac{e^{\gamma\delta}}{\Gamma(1-\delta)} x \prod_{\substack{y < p \leq x \\ p \in Q}} \left(1 - \frac{1}{p}\right) (1 + O(D)),$$

where $D := \frac{\ln(y)}{\ln(x)} + \ln^{-B}(y)$ and $B := \min(A, 1)$.

It is possible to choose the integer k big enough in order to verify the following equality

$$\sum_{\substack{p \leq x \\ p \in Q}} \ln(p) = O((y + kP_Q) \ln^{-A}(y + kP_Q)),$$

where the value δ equals to zero and $A > 1$.

Therefore, it implies that

$$\Psi(x + kP_Q, y, Q) = (x + kP_Q) \prod_{\substack{y < p \leq x \\ p \in Q}} \left(1 - \frac{1}{p}\right) (1 + O(D_1)),$$

and

$$\Psi(y + kP_Q, y, Q) = (y + kP_Q) \prod_{\substack{y < p \leq x \\ p \in Q}} \left(1 - \frac{1}{p}\right) (1 + O(D_2)).$$

Then we can find for k big enough that

$$\begin{aligned} \Psi(x + kP_Q, y, Q) - \Psi(y + kP_Q, y, Q) &= (x - y) \prod_{\substack{y < p \leq x \\ p \in Q}} \left(1 - \frac{1}{p}\right) \left(1 + O\left(\frac{1}{\ln(y)}\right)\right) \\ &= \Psi(x, y, Q) - y. \end{aligned}$$

Then it concludes that

$$\Psi(x, y, Q) = (x - y) \prod_{\substack{y < p \leq x \\ p \in Q}} \left(1 - \frac{1}{p}\right) \left(1 + O\left(\frac{1}{\ln(y)}\right)\right) + y.$$

9.4 Proof of the fourth part of Lemma 3.6

To Prove the last point of the Lemma 3.6, it suffices to notice that $p_i \sim i \ln(i)$ in order to quantify the $\prod_{\substack{y < p \leq x \\ p \in Q}} \left(1 - \frac{1}{p}\right)$ by simple integration as follows

$$\begin{aligned}
\prod_{\substack{y < p \leq x \\ p \in Q}} \left(1 - \frac{1}{p}\right) &= \exp \left(\sum_{\substack{y < p \leq x \\ p \in Q}} \ln \left(1 - \frac{1}{p}\right) \right) \\
&= \exp \left(\sum_{i=y/\ln(y)}^{x/\ln(x)} \ln \left(1 - \frac{1}{i \ln(i)}\right) \right) \\
&\sim \exp \left(\sum_{i=y/\ln(y)}^{x/\ln(x)} \left(-\frac{1}{i \ln(i)}\right) \right) \\
&\sim \exp \left(\int_{y/\ln(y)}^{x/\ln(x)} \left(-\frac{1}{w \ln(w)}\right) dw \right) \\
&\sim \frac{\ln(y)}{\ln(x)}.
\end{aligned}$$

■

10 Proof of the conjecture of Goldbach

To prove the conjecture that said that all even number can be written as difference or sum of two prime numbers. Lemma 3.5 will be the main idea to conclude the conjecture. The question will be about the possibility to find k such that

$$p_{n+1} \leq \left(2 \prod_{i=1}^{n-k+1} p_i\right) \leq p_{n+1}^2, \quad (24)$$

in order to make sure that all integers inside the set $U_{\prod_{i=1}^{n-k+1} p_i}^{k,2}$ are primes.

For n big enough, we have that $p_n \sim n \ln(n)$ see [1], so

$$\prod_{i=1}^{n-k} p_i \sim \exp \left(\sum_{i \leq n-k} \ln(p_i) \right) \sim \exp \left(\sum_{i \leq n-k} \ln(i \ln(i)) \right),$$

then we can find the following approximation

$$\prod_{i=1}^{n-k} p_i \sim \exp((n-k) \ln(n-k))$$

This result can be calculated by using stirling formula.

In order to find k as an increased and not bounded function of n , the following inequality needs to be solved

$$(n+1) \ln(n+1) \leq \exp((n-k) \ln(n-k)) \leq (n+1)^2 \ln^2(n+1).$$

In order to make sure that all values in $U_{\prod_{i=1}^{n-k+1} p_i}^k$ are prime numbers and their difference form all even numbers less than $\prod_{i=1}^{n-k+1} p_i$, the last inequality must be satisfied, then it is possible to choose

$$k \sim n - \frac{3 \ln(n)}{2 \ln(\ln(n))},$$

or in general as $n - f(n)$ where $f(n)^{f(n)} \sim n^\alpha$, for $\alpha \in (1, 2)$, in order to get

$$\exp((n-k) \ln(n-k)) \sim n^\alpha.$$

Till now we have proved that the difference of prime number forms all even number, therefore to prove that the sum of prime numbers form also all even number from the proof of the difference of prime number forms all even number it is enough to show that en mode of $\prod_{i=1}^n p_i$ we have

$$\Delta V_{\prod_{i=1}^n p_i} = V_{\prod_{i=1}^n p_i} + V_{\prod_{i=1}^n p_i},$$

which it is trivial by using the fact that for all $x \in V_{\prod_{i=1}^n p_i}$ implies that $\prod_{i=1}^n p_i - x \in V_{\prod_{i=1}^n p_i}$, i.e.,

$$\begin{aligned} (\Delta V_{\prod_{i=1}^n p_i})_{\text{mod}(\prod_{i=1}^n p_i)} &= \left(\Delta V_{\prod_{i=1}^n p_i} + \prod_{i=1}^n p_i \right)_{\text{mod}(\prod_{i=1}^n p_i)} \\ &= \left(V_{\prod_{i=1}^n p_i} - V_{\prod_{i=1}^n p_i} + \prod_{i=1}^n p_i \right)_{\text{mod}(\prod_{i=1}^n p_i)} \\ &= (V_{\prod_{i=1}^n p_i} + V_{\prod_{i=1}^n p_i})_{\text{mod}(\prod_{i=1}^n p_i)}. \end{aligned}$$

■

11 Proof of the conjecture of twin prime

In this section I will prove the conjecture by two different ways, the first prove it is just a sequences of the lemma 3.5 directly. The second one shows my first ideas when I started to find the proof of the twin number conjecture.

11.1 First Approach

The lemma 3.5 stats that

$$\left(\Delta U_{\prod_{i=1}^{n+1} p_i}^k\right) \supseteq \left[0 : 2 : \prod_{i=1}^{n-k+1} p_i - 2\right],$$

where $U_{\prod_{i=1}^{n+1} p_i}^k = V_{\prod_{i=1}^{n+1} p_i} \cap \left[0, 2\prod_{i=1}^{n-k+1} p_i\right]$.

Since the set $U_{\prod_{i=1}^{n+1} p_i}^k$ contains only co-primes numbers with all the first $n+1$ primes numbers, the two smallest values inside the set are 1 and p_{n+2} . Therefore, to ensure that the set $U_{\prod_{i=1}^{n+1} p_i}^k$ contains only primes number, it is enough to choose k around $n - \frac{\ln(n)}{\ln(\ln(n))}$ in order to ensure that the biggest co-prime inside $U_{\prod_{i=1}^{n+1} p_i}^k$ is less than p_{n+1}^2 .

Since the boundaries of the set $U_{\prod_{i=1}^{n+1} p_i}^k$, without considering the value 1, are going to infinity when n goes to infinity, the existence of infinity twin number is verified

Since there is no prime between two primes that defer by 4, so the same proof can be conducted easily in order to prove the existence of infinitely couples of primes such that $p_{n+1} - p_n = 4$, for every integer k . we can conclude further that $p_n = 6k + 1$ and $p_{n+1} = 6k + 5$ in modulo 6.

$$\liminf_{n \rightarrow \infty} (p_{n+1} - p_n) = 2.$$

■

11.2 Second Approach

The proof will use the both previous lemmas and the following concepts:

Firstly: $\lim_{n \rightarrow \infty} \pi(p_{n+1}^2) - \pi(p_{n+1}) = \infty$, where $\pi(x)$ is the prime counting function i.e., number of primes less than x . (see [1] and [2])

Secondly: The existence solution for the following equation

$$x \left(\prod_{i=1}^n p_i \right) + yp_{n+1} = 2,$$

where $x \in \Delta[1 : p_{n+1} - 1]$ and $y \in \Delta V_{\prod_{i=1}^n p_i}$.

For n big enough, We need to prove the existence of twin primes q and $q + 2$ that belongs to

$$V_{\prod_{i=1}^n p_i} \cap [p_n, p_{n+1}^2[.$$

Referring to Theorem 3.1, $\forall x \in V_{\prod_{i=1}^n p_i}$ and $x < p_{n+1}^2$ then x is a prime number.

To prove the conjecture it is enough to show, for all n big enough, that

$$\exists (q, q + 2) \in \left(V_{\prod_{i=1}^n p_i} \cap [p_n, p_{n+1}^2] \right)^2.$$

Suppose that x_1 and x_2 belong to $V_{\prod_{i=1}^{n+1} p_i}$ so it exists $(l_1, l_2) \in [1 : p_{n+1} - 1]^2$ and $(cp_1, cp_2) \in (V_{\prod_{i=1}^n p_i})^2$ such that for all $(m_1, m_2) \in \mathbb{Z}^2$ we have

$$\begin{cases} x_1 = \left(\prod_{i=1}^n p_i \right) l_1 + p_{n+1} cp_1 + m_1 \left(\prod_{i=1}^{n+1} p_i \right) \\ x_2 = \left(\prod_{i=1}^n p_i \right) l_2 + p_{n+1} cp_2 + m_2 \left(\prod_{i=1}^{n+1} p_i \right) \end{cases} \quad (25)$$

Abstracting both equations at the system 25, we get

$$x_2 - x_1 = \left(\prod_{i=1}^n p_i \right) (l_2 - l_1) + p_{n+1} (cp_2 - cp_1) + (m_2 - m_1) \left(\prod_{i=1}^{n+1} p_i \right),$$

and if x_1 and x_2 are twin primes then

$$2 + (m_1 - m_2) \left(\prod_{i=1}^{n+1} p_i \right) = \left(V_{\prod_{i=1}^n p_i} \right) (l_2 - l_1) + p_{n+1} (cp_2 - cp_1)$$

By introducing the mod, we obtain

$$2 = \left(\left(V_{\prod_{i=1}^n p_i} \right) (l_2 - l_1) + p_{n+1} (cp_2 - cp_1) \right)_{\text{mod} \left(V_{\prod_{i=1}^{n+1} p_i} \right)}. \quad (26)$$

All parameters in equation 26 need to be calculated and to show that both x_1 and x_2 are primes by showing their belong to the interval $[p_n; p_{n+1}^2[$.

Let denote $\Delta l = l_2 - l_1$ and $\Delta cp = cp_2 - cp_1$. From lemma 3.3 we have

$$\begin{cases} \Delta cp \in [0 : 2 : \prod_{i=1}^n p_i - 2] \\ \Delta l \in [2 - p_{n+1} : p_{n+1} - 2] \end{cases} \quad (27)$$

The equation 26 can be written as follows:

$$2 + m' \prod_{i=1}^{n+1} p_i = \left(\left(\prod_{i=1}^n p_i \right) \Delta l + p_{n+1} \Delta cp \right). \quad (28)$$

By dividing the previous equation 28 by 2, we get the following

$$1 + m' \prod_{i=3}^{n+1} p_i = \left(\left(\prod_{i=3}^n p_i \right) \Delta l + p_{n+1} \frac{\Delta cp}{2} \right). \quad (29)$$

According to Diophantine theorem, the equation 29 has a particular solution, it means $\exists \Delta l^*$ and Δcp^* such that

$$2 + m' \prod_{i=1}^{n+1} p_i = \left(\left(\prod_{i=1}^n p_i \right) \Delta l^* + p_{n+1} \Delta cp^* \right)$$

Then the general solution will be under the following form

$$\begin{cases} \Delta cp = \Delta cp^* + k \prod_{i=1}^n p_i \\ \Delta l = \Delta l^* + kp_{n+1} \end{cases} \quad (30)$$

where $k \in \mathbb{Z}$.

We need to check if it exists k such that

$$\begin{cases} 2 - p_{n+1} \leq \Delta l \leq p_{n+1} - 2 \\ \text{and} \\ \Delta cp \in [0 : 2 : \prod_{i=1}^n p_i - 2]. \end{cases} \quad (31)$$

It is obvious to see that for all $\Delta l^* \in \mathbb{Z}$, it exists k such that $\Delta l^* + kp_{n+1} \in [2 - p_{n+1}, p_{n+1} - 2]$, because if $(\Delta l^*)_{\text{mod}(p_{n+1})} = r$ then k can be chosen accordingly

$$\begin{cases} \text{if } r = p_{n+1} - 1 \Rightarrow k = \left\lfloor -\frac{\Delta l^*}{p_{n+1}} \right\rfloor - 1 \\ \text{if } r \in [0, p_{n+1} - 2] \Rightarrow k = \left\lfloor -\frac{\Delta l^*}{p_{n+1}} \right\rfloor. \end{cases} \quad (32)$$

Still to check the possibility that

$$\Delta cp \in [0 : 2 : \prod_{i=1}^n p_i - 2],$$

for that let start with the first condition about Δl that

$$2 - p_{n+1} \leq \Delta l^* + kp_{n+1} \leq p_{n+1} - 2,$$

By multiplication all parts by $\prod_{i=1}^n p_i$ we get

$$2 \prod_{i=1}^n p_i - \prod_{i=1}^{n+1} p_i \leq \prod_{i=1}^n p_i \Delta l^* + k \prod_{i=1}^{n+1} p_i \leq \prod_{i=1}^{n+1} p_i - 2 \prod_{i=1}^n p_i.$$

Indeed, it follows from equation 28 that $2 = ((\prod_{i=1}^n p_i) \Delta l^* + p_{n+1} \Delta cp^*) - k_0(\prod_{i=1}^{n+1} p_i)$ then

$$2 \prod_{i=1}^n p_i - \prod_{i=1}^{n+1} p_i \leq (2 - p_{n+1} \Delta cp^*) + (k + k_0) \prod_{i=1}^{n+1} p_i \leq \prod_{i=1}^{n+1} p_i - 2 \prod_{i=1}^n p_i,$$

therefore

$$\frac{2 \prod_{i=1}^n p_i - 2}{p_{n+1}} - \prod_{i=1}^n p_i \leq -\Delta cp^* + (k + k_0) \prod_{i=1}^n p_i \leq \frac{-2 \prod_{i=1}^n p_i + 2}{p_{n+1}} + \prod_{i=1}^n p_i.$$

For all even possible value of Δcp^* , we can find k_0 in order to make sure that $\Delta cp \in [0 : 2 : \prod_{i=1}^n p_i - 2]$.

Finally x_1 and x_2 can be written as

$$\begin{cases} x_1 = (\prod_{i=1}^n p_i) l_1 + p_{n+1} cp_1 + m_1 \left(\prod_{i=1}^{n+1} p_i \right) \\ x_2 = (\prod_{i=1}^n p_i) (\Delta l^* + l_1) + p_{n+1} (\Delta cp^* + cp_1) + m_2 \left(\prod_{i=1}^{n+1} p_i \right) \end{cases} \quad (33)$$

Another question is raised to check and verify again the following

$$\begin{cases} (\Delta l^* + l_1)_{\text{mod}(\prod_{i=1}^n p_i)} \in [1 : p_{n+1} - 1] \\ \text{and} \\ (\Delta cp^* + cp_1)_{\text{mod}(\prod_{i=1}^n p_i)} \in V_{\text{mod}(\prod_{i=1}^n p_i)} \end{cases} \quad (34)$$

From Theorem 3.1, we need to be sure that $\Delta l^* + l_1$ and p_{n+1} are co-primes and also $\Delta cp^* + cp_1$ is co-prime with $\prod_{i=1}^n p_i$. To do that, we can see that Δl^* is co-prime with p_{n+1} and $\Delta cp^*/2$ is co-prime with $\prod_{i=3}^n p_i$, then l_1 can be chosen easily in order to avoid that $(\Delta l^* + l_1)_{\text{mod}(\prod_{i=1}^n p_i)} = 0$.

The only question of the existence of cp_1 such that $cp_1 \in V_{\prod_{i=3}^n p_i}$, $\Delta cp^* + cp_1 \in V_{\prod_{i=1}^n p_i}$, and $x_1 \in (p_{n+1}, p_{n+1}^2)$ needs to be answer in order to finish the prove of the conjecture.

It was proved that gap between primes is finite,[5], by consequence for n big enough, $n \sim p_{[\Pi(n)]}$, then by substitution the variable n by $n \ln(n)$, we get very interesting formula

$$p_n \sim n \ln(n).$$

Number of prime numbers less than n can be calculated differently by

$$\pi(n) = n - \text{card} \left(\bigcup_{i=2}^n A_i \right) = n - \left(\sum_{k=2}^n (-1)^k \text{card} \left(\bigcap_{i=2}^k A_i \right) \right),$$

where $A_i = \{m : m \in [i+1, n] \text{ and } m_{\text{mod}(i)} = 0\}$, in our next paper, a new method in how to estimate $\pi(n)$ will be our focus, here are some headline

$$\begin{aligned}
\pi(n) &= n - \left(\sum_{k=2}^n (-1)^k \text{card} \left(\bigcap_{i=2}^k A_i \right) \right) \\
&= n - \left(\sum_{k=2}^n (-1)^k \sum_{2 \leq i_1 < i_2 < \dots < i_k \leq n} \left(\text{card} \left(\left\lfloor \frac{n}{\prod_{i=2}^k n_i} \right\rfloor - 1 \right) \right) \right) \\
&= n - \left(\sum_{k=2}^n (-1)^k \sum_{2 \leq i_1 < i_2 < \dots < i_k \leq n} \left(\text{card} \left(\left\lfloor \frac{n}{\prod_{i=2}^k n_i} \right\rfloor \right) \right) \right) - 1 \\
&\approx n \prod_{i=2}^n \left(1 - \frac{1}{i} \right) \\
&\approx \frac{n}{\ln(n)}.
\end{aligned}$$

Furthermore, the existence of several choices of cp_1 such that $\Delta cp^* + cp_1 \in V_{\prod_{i=1}^n p_i}$ is assured by Lemma 3.5. The value of Δcp^* will be successively divided by $\prod_{i=1}^n p_i$ as follows:

$$\begin{aligned}
\Delta cp^* &= l_1 \prod_{i=1}^{n-1} p_i + r_1 \\
r_1 &= l_2 \prod_{i=1}^{n-2} p_i + r_2 \\
&\vdots \\
r_{k-1} &= l_k \prod_{i=1}^{n-k} p_i + r_k
\end{aligned}$$

where r_i and l_i are the quotients and reminders of each division. Then Δcp^* can be written as follows:

$$\Delta cp^* = r_k + \sum_{j=1}^k l_j \left(\prod_{i=1}^{n-j} p_i \right)$$

The value of k should be chosen in order to be sure that x_1 belongs to the interval of primes number only, $[p_{n+1}, p_{n+1}^2) \cap V_{\prod_{i=1}^{n+1} p_i}$. To do so k needs to be the first value that verified the following inequality:

$$\left(\prod_{i=1}^{n-k} p_i \right) \leq \frac{p_{n+1}}{2}.$$

From the part b of Lemma 3.3, it is clear that it exists an integer j , strictly positive, for which

$$cp_1 \in \left[\frac{j \prod_{i=1}^n p_i}{p_{n+1}}, \frac{j \prod_{i=1}^n p_i}{p_{n+1}} + p_{n+1} \right) \cap V_{\prod_{i=1}^{n+1} p_i},$$

and another co-prime number, $cp_2 \in V_{\prod_{i=1}^{n+1} p_i}$ such that $\Delta cp^* = cp_2 - cp_1$

We are sure now about the possibility of selecting the right l_1 in order to make sure that x_1 is a prime number by assuring that x_1 is inside the interval $[p_{n+1}, p_{n+2}^2) \cap V_{\prod_{i=1}^{n+1} p_i}$.

Since there is no prime between two primes that defer by 4, so the same proof can be conducted easily in order to prove the existence of infinitely couples of primes such that $p_{n+1} - p_n = 4$, for every integer k . we can conclude also that $p_n = 1$ in modulo 6.

■

12 Appendix

In this section, new approach in how to calculate the density of co-primes will be described. Let's suppose that for all integer $x > p_n$ we have for $Q_m = \{p_i \mid n \leq i < n + m\}$ and p_N represent the biggest prime less than x

$$\Psi(x, p_{n-1}, Q_m) = x \prod_{i=n}^{n+m-1} \left(1 - \frac{1}{p_i} \right) + O(f(x, m)), \text{ for all } m \leq N - n.$$

Using the proof by induction, the function $f(x, m)$ can be estimated as a linear function with $\ln(m + n)$.

For $m = 1$, we have

$$\begin{aligned} \Psi(x, p_{n-1}, Q_1) &= x \prod_{i=n}^n \left(1 - \frac{1}{p_i} \right) + O(f(x, 1)) \\ &= x - \frac{x}{p_n} + O(f(x, 1)), \end{aligned}$$

The error function, $O(f(x, 1))$, can be calculated easily as follows

$$\begin{aligned}
O(f(x, 1)) &= x - \left\lfloor \frac{x}{p_n} \right\rfloor - \left(x - \frac{x}{p_n} \right) \\
&= \frac{x}{p_n} - \left\lfloor \frac{x}{p_n} \right\rfloor \\
&\leq 1.
\end{aligned}$$

Let's assume that

$$\Psi(x, p_{n-1}, Q_m) = x \prod_{i=n}^{n+m-1} \left(1 - \frac{1}{p_i} \right) + O(f(x, m))$$

and we need to show

$$\Psi(x, p_{n-1}, Q_{m+1}) = x \prod_{i=n}^{n+m} \left(1 - \frac{1}{p_i} \right) + O(f(x, m+1)).$$

Let A_i be set of multiple of p_{n+i} and less than x , $A_i = \{i \mid \gcd(i, p_{n+i-1}) = p_{n+i-1} \text{ and } i \leq x\}$, then

$$\begin{aligned}
\Psi(x, p_{n-1}, Q_{m+1}) &= x - \text{card} \left(\bigcup_{i=1}^{m+1} A_i \right) \\
&= x - \text{card} \left(\left(\bigcup_{i=1}^m A_i \right) \cup A_{m+1} \right) \\
&= x - \text{card} \left(\left(\bigcup_{i=1}^m A_i \right) \right) - \text{card}(A_{m+1}) + \text{card} \left(\left(\bigcup_{i=1}^m A_i \right) \cap A_{m+1} \right) \\
&= x - \text{card} \left(\left(\bigcup_{i=1}^m A_i \right) \right) - \left\lfloor \frac{x}{p_{n+m}} \right\rfloor + \text{card} \left(\left(\bigcup_{i=1}^m A_i \right) \cap A_{m+1} \right).
\end{aligned}$$

Note that $A_i \cap A_{m+1} = \{i \mid \gcd(i, p_{n+m} p_{n+i-1}) = p_{n+m} p_{n+i-1} \text{ and } i \leq x\}$ and $\Psi(x, p_{n-1}, Q_m) = x - \text{card} \left(\left(\bigcup_{i=1}^m A_i \right) \right)$ then

$$\begin{aligned}
\Psi(x, p_{n-1}, Q_{m+1}) &= \Psi(x, p_{n-1}, Q_m) - \left\lfloor \frac{x}{p_{n+m}} \right\rfloor + \frac{x}{p_{n+m}} - \Psi \left(\frac{x}{p_{n+m}}, p_{n-1}, Q_m \right) \\
&= x \prod_{i=n}^{n+m-1} \left(1 - \frac{1}{p_i} \right) - \left\lfloor \frac{x}{p_{n+m}} \right\rfloor + \frac{x}{p_{n+m}} - \frac{x}{p_{n+m}} \prod_{i=n}^{n+m-1} \left(1 - \frac{1}{p_i} \right) \\
&\quad + O(f(x, m) - f(x/p_{n+m}, m)) \\
&= x \prod_{i=n}^{n+m} \left(1 - \frac{1}{p_i} \right) + O(f(x, m) - f(x/p_{n+m}, m) + 1)
\end{aligned}$$

In order to force the last formula to correct we have to find the function, f , that verify the following

$$f(x, m) + f(x/p_{n+m}, m) = f(x, m+1) + O(1).$$

For n is big enough integer, then

$$\begin{aligned} -f(x/p_{n+m}, m) &= f(x, m+1) - f(x, m) \\ &\sim \frac{\partial f(x, m)}{\partial m} \end{aligned}$$

Since $p_{n+m} \sim (n+m) \ln(n+m)$ then differential equation needs to be solved

$$\frac{\partial f(x, m)}{\partial m} = -f\left(\frac{x}{(n+m) \ln(n+m)}, m\right).$$

The function

$$f(x, m) \sim \frac{x}{\ln(x) \ln(n+m)}$$

is a possible because

$$\begin{aligned} \frac{x}{\ln(x) \ln(n+m)} - \frac{x/p_{n+m}}{\ln(x/p_{n+m}) \ln(n+m)} &= \frac{x}{\ln(x)} \left(\frac{1}{\ln(n+m)} \right) \\ &\quad - \left(\frac{x}{(n+m) \ln(x) \ln^2(n+m) (1 + \ln(n+m)/\ln(x))} \right) \\ &\leq \frac{x}{\ln(x)} \left(\frac{1}{\ln(n+m)} - \frac{1}{2(n+m) \ln^2(n+m)} \right) \\ &\leq \frac{x}{c \ln(x) \ln(n+m+1)} \\ &\leq f(x, m+1) \end{aligned}$$

where c is a fixed constant bigger than one. then

$$\Psi(x, p_{n-1}, Q_m) = x \prod_{i=n}^{n+m-1} \left(1 - \frac{1}{p_i} \right) + O\left(\frac{x}{\ln(x) \ln(n+m)} \right), \text{ for all } m \leq N-n.$$

For n big enough we can write

$$\Psi(x, p_{n-1}, Q_{N-n}) = x \frac{\ln(n)}{\ln(x)} + O\left(\frac{x}{\ln^2(x)} \right).$$

■

References

- [1] G. H. Hardy and E. M. Wright, An introduction to the theory of numbers, Oxford University Press, 1979. ISBN 0198531702. MR 81i:10002 (Annotation available)
- [2] "PrimeGrid's Challenge Series - 2008 Final Standings". PrimeGrid. Retrieved 2011-09-19.
- [3] Daniel Shanks and John W. Wrench, Jr. "Brun's constant", *Mathematicis of computation*, Volume 28, Number 125, Januaray 1974.
- [4] James Maynard, "Small gaps between primes" *Annals of Mathematics* Pages 383-413 from Volume 181 (2015),
- [5] Y Zhang, "Bounded gaps between primes", *Annals of Mathematics*, 2013.Pages 1121-1174 from Volume **179**, (2014)
- [6] Leonard E. Dickson, History of the Theory of Numbers, Vol. 1, Chelsea Publishing Co., New York, 1971
- [7] Goldbach Conjecture, World Scientific Publishing Co., Singapore, 1984
- [8] Daniel Shanks, Solved and Unsolved Problems in Number Theory, 3rd edition, Chelsea Publishing Co., New York, 1985
- [9] Paulo Ribenboim, The Book of Prime Number Records, 2nd edition, Springer-Verlag Inc., New York, 1989
- [10] Richard W., "Sievinh by large Prime Factors", *Mh. Math*, 109, 247-256 (1990).
- [11] Goldston, D. A., McCurley, K. S. : Sieving the integers by large primes. *J. Number Theory*, 28, 94-115 (1998).